

# 全国保健医療情報ネットワークの構築に向けた 相互接続基盤実証について

平成30年4月19日  
総務省

# 医療等分野の相互接続基盤の在り方に関する実証

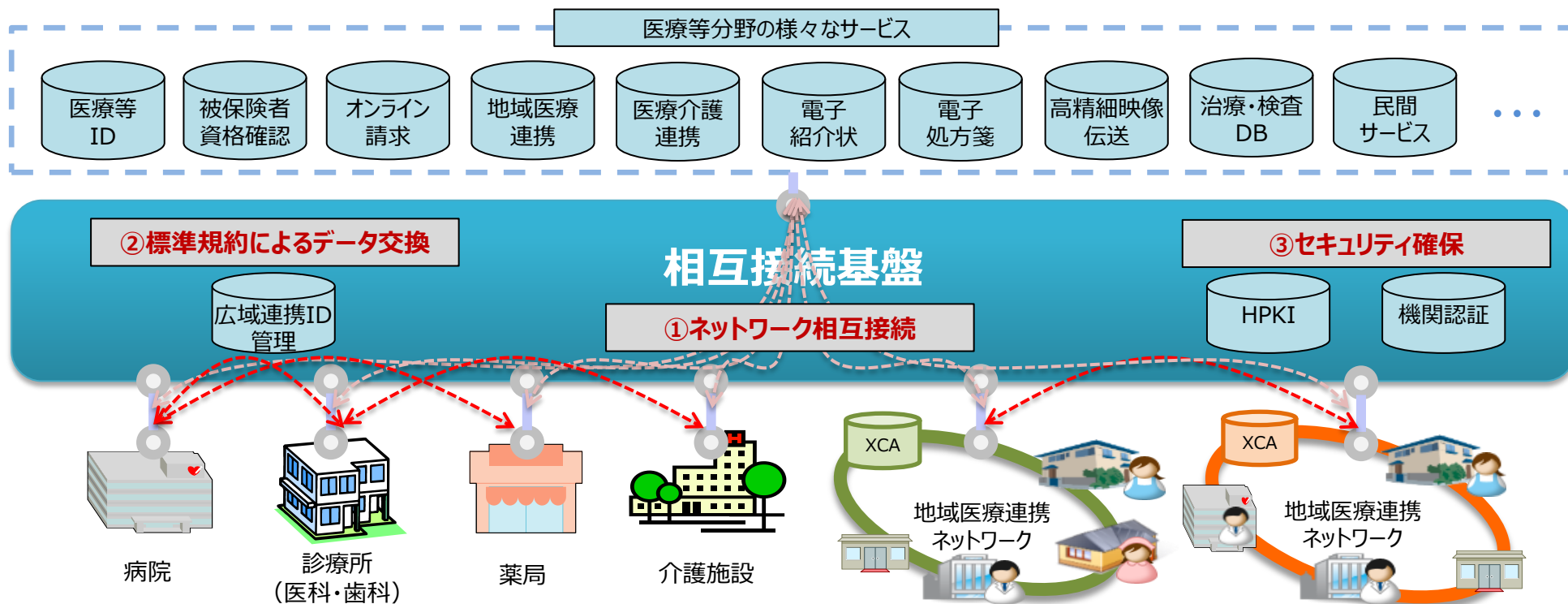
- 2020年の「全国保健医療情報ネットワーク」構築に向けて、医療等分野のデータ共有基盤（**相互接続基盤**）の在り方の実証事業を実施。
- 本事業を通じ、「**①ネットワークの相互接続**」、共通ルールに基づき患者情報を流通させるための「**②標準規約によるデータ交換**」、安全な通信を実現するための「**③セキュリティ確保**」について検討し、実運用フェーズに移行するための運用ルール等を策定。

## <現状の課題>

医療等分野においては、これまで目的別、地域別にネットワークが構築されており、今後見込まれる様々な医療等分野のICTサービスを共通利用するための高度なセキュリティが確保されたネットワークが存在しない。

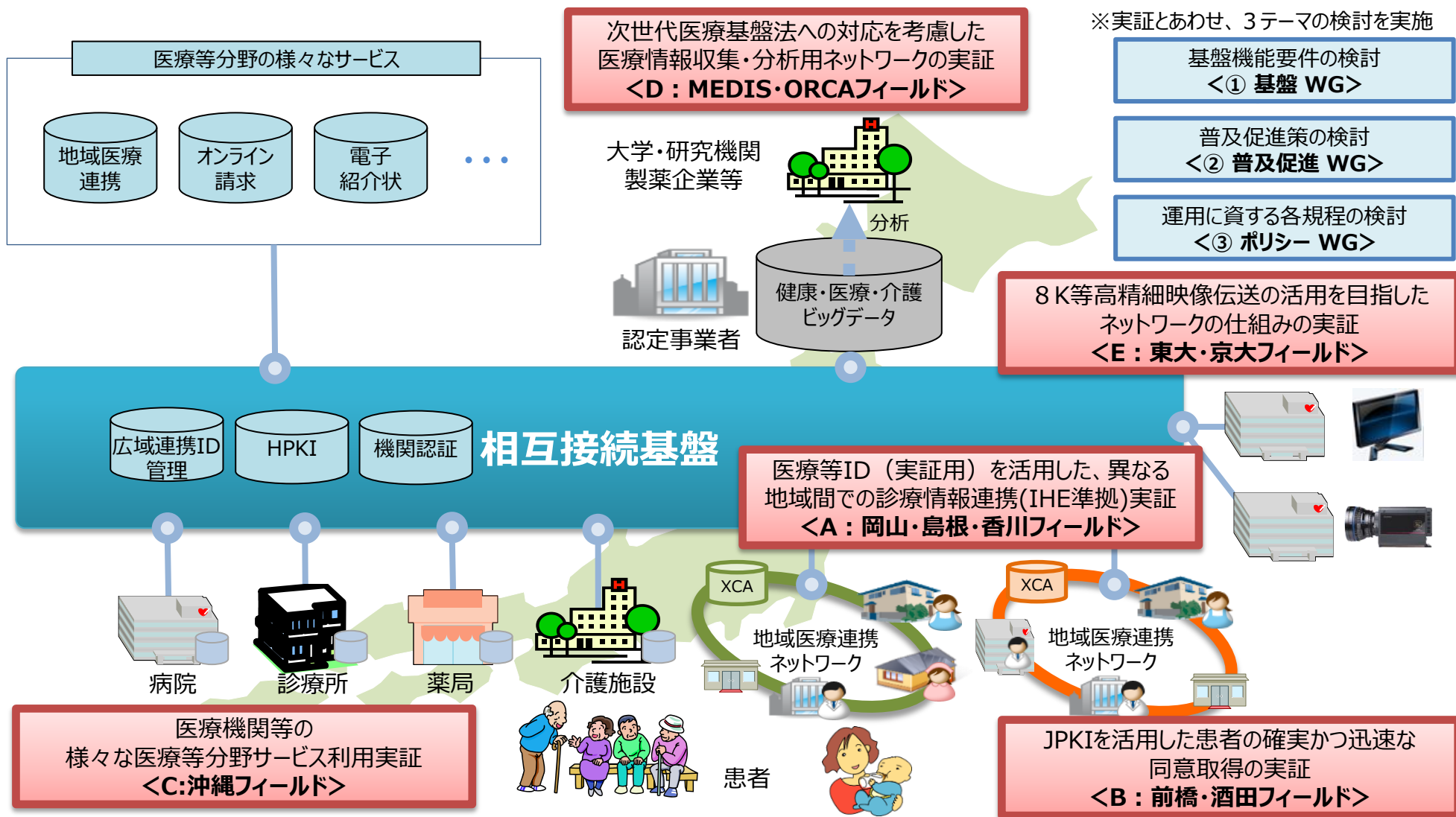
## <基本コンセプト>

- 安心安全なネットワーク** 厳格な認証のもとに、医療情報を安心して流通可能
- 全体最適化されたネットワーク** 医療等分野の様々なサービスを共通利用可能
- ユニバーサルサービスとしてのネットワーク** 公益性を担保し全国をカバー



# 相互接続基盤モデルの実証フィールド

- テーマ別に3つの検討WG「①基盤」、「②普及促進」、「③ポリシー」、および、5つのフィールド実証WG「A:岡山・島根・香川」、「B:前橋・酒田」、「C:沖縄」、「D:MEDIS・ORCA」、「E:東大・京大」にて、検証を実施。



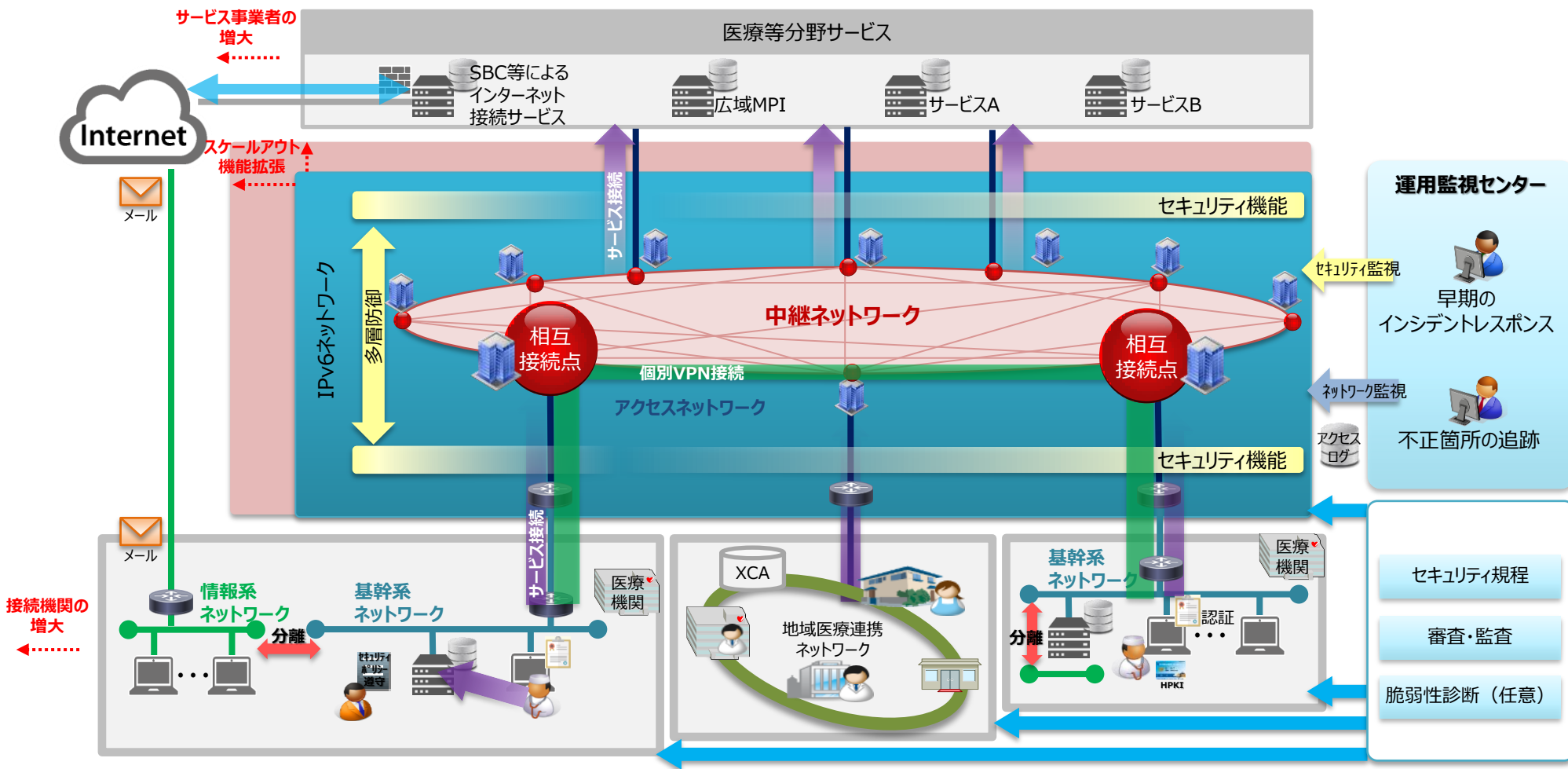
# 相互接続基盤の全体像

## <ネットワーク>

- IPv6を採用し、医療機関等を接続する「アクセスネットワーク」と相互接続点を接続する「中継ネットワーク」に階層化
- 接続機関やサービス事業者等の増大に応じたスケールアウト、需要に応じた機能拡張

## <セキュリティ>

- 多層防御、セキュリティ監視、インシデントレスポンスによる、防御、被害の最小化、脅威の排除
- 接続する施設や個人を認証、セキュリティ規程遵守、審査・監査、および脆弱性診断（任意）による接続機関の予防保全

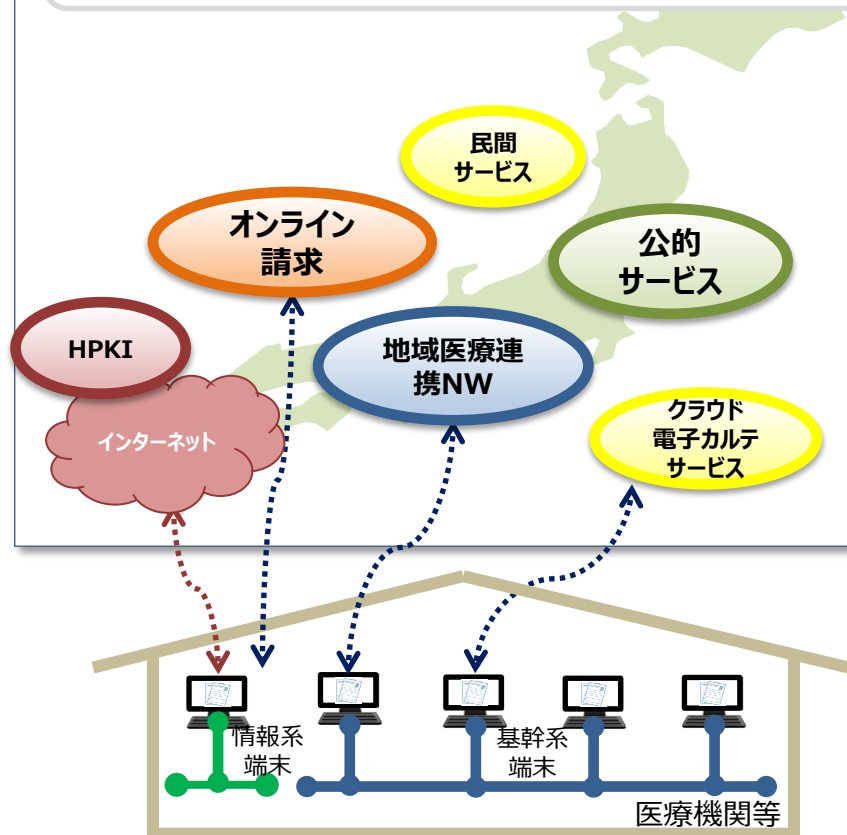


# 相互接続基盤の導入意義

- これまで医療等分野においては、地域別や目的別に、その都度ネットワークが構築され、全体最適の観点で必ずしも効率的でなく、医療機関等においても、コスト、セキュリティ、業務効率性に課題。
- 今後、更なる医療ICT政策を加速するうえでは、統一ポリシーに基づき運用され、一定のセキュリティが確保された「相互接続基盤」が、上記課題を解決する有効な方策であることを本実証において示した。

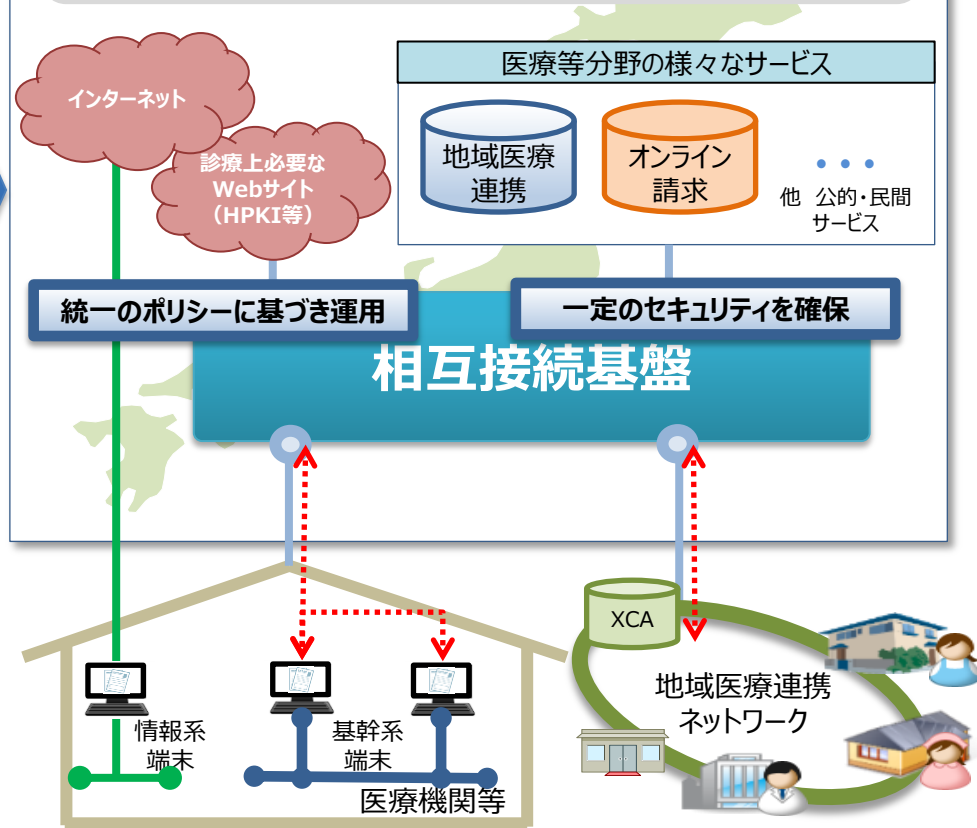
## 現状課題

- 用途別に回線や端末を用意し、医療等分野の各サービス毎にアクセス、データ移動や情報のコピー＆ペーストの手間が発生、業務が分断
- 外部接続に対するセキュリティ不安有



## 相互接続基盤による解決策

- 回線1本、端末共用で様々な医療等分野のサービスを共通利用、業務の分断が解消でき、業務効率化や利便性向上
- 相互接続基盤のみに外部接続が限定されることで安心安全



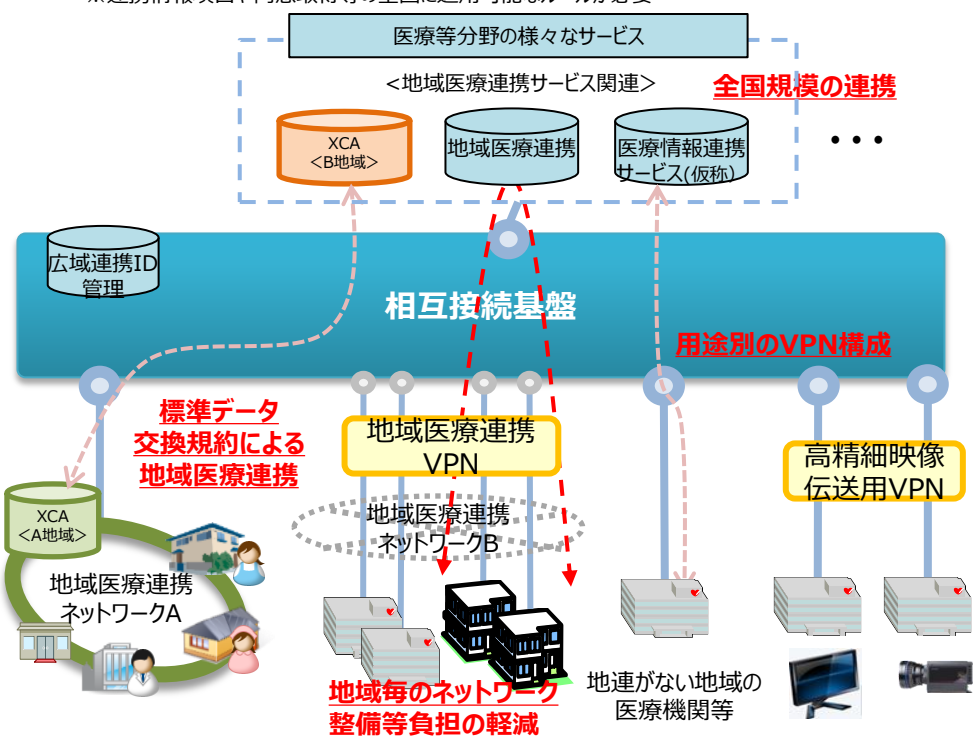
# 相互接続基盤によって可能になること

- 相互接続基盤は、「安心安全（高セキュリティ）」、「全体最適（低コスト）」、「公益性担保（全国をカバー）」の3つの基本コンセプトを満たし、「①医療機関間連携」、「②医療等分野サービスの共通利用」を実現。

## ①医療機関間連携

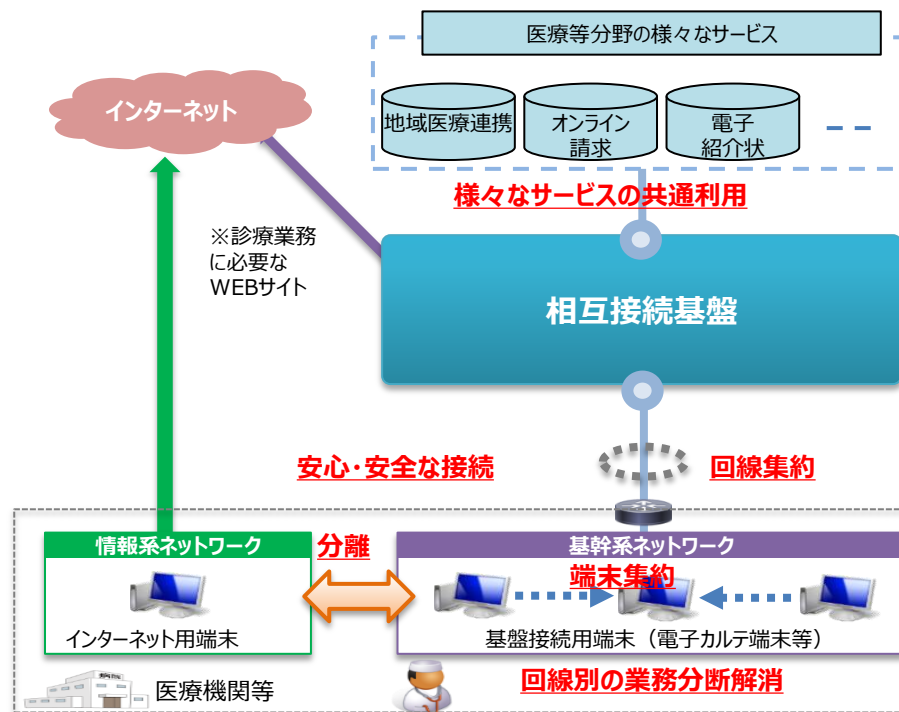
- 医療機関間の通信に加え、地域医療連携ネットワークのインフラとしてもVPNを構成でき、地域毎のネットワーク整備・維持やポリシー策定の負担が軽減される。
- 地域医療連携ネットワークがない地域の医療機関も含めた、全国規模の診療情報連携が可能になる。

※連携情報項目や同意取得等の全国に適用可能なルールが必要



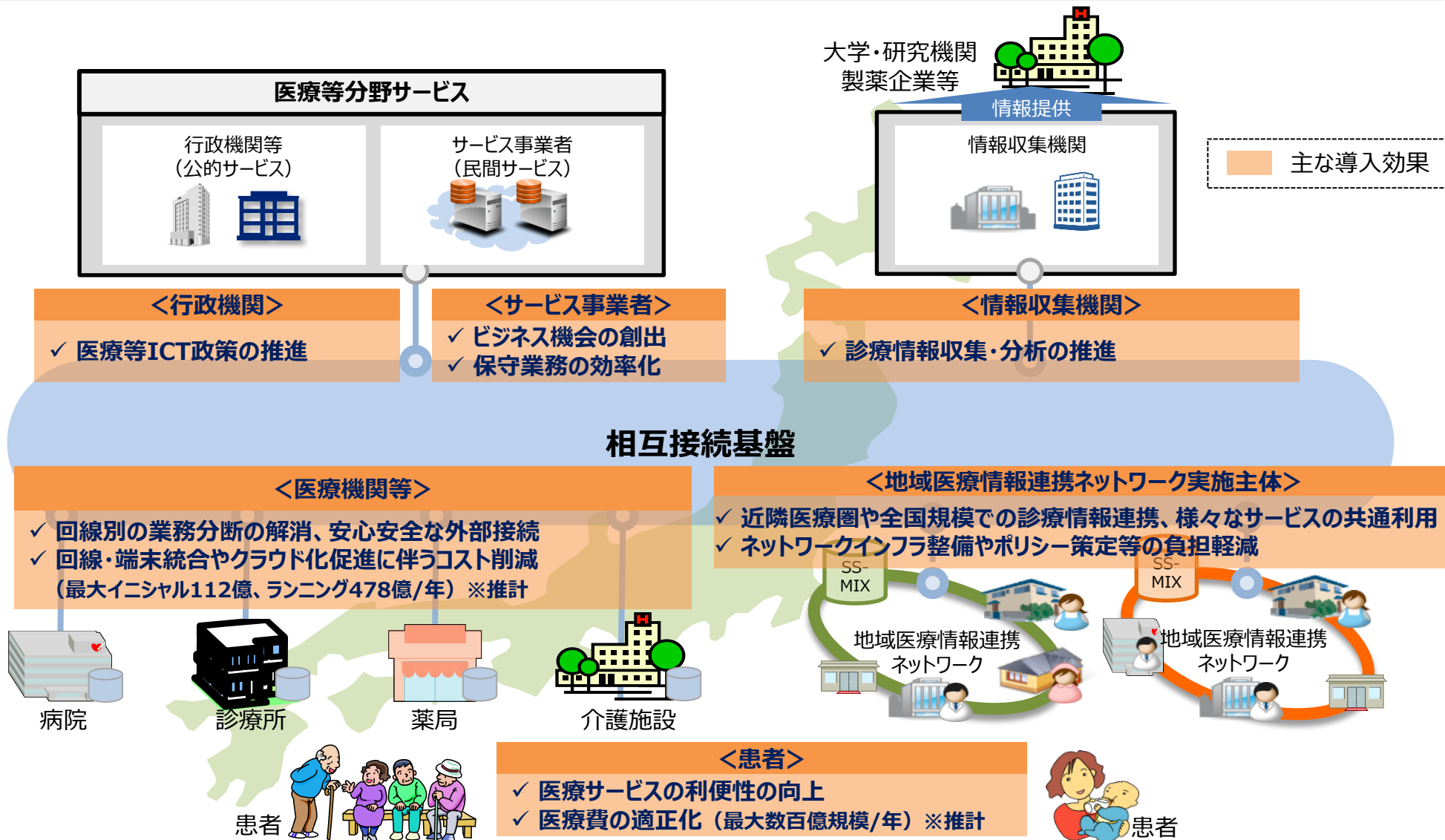
## ②医療等分野サービスの共通利用

- 医療機関等から、医療等分野の様々なサービスを共通利用でき、回線別の業務分断が解消。また、回線・端末等の集約効果が見込める。
- 統一ポリシーに基づき運用され、一定のセキュリティレベルが確保された相互接続基盤のみに外部接続が限定されることにより、安心安全に接続できる。



# ステークホルダー別の導入効果

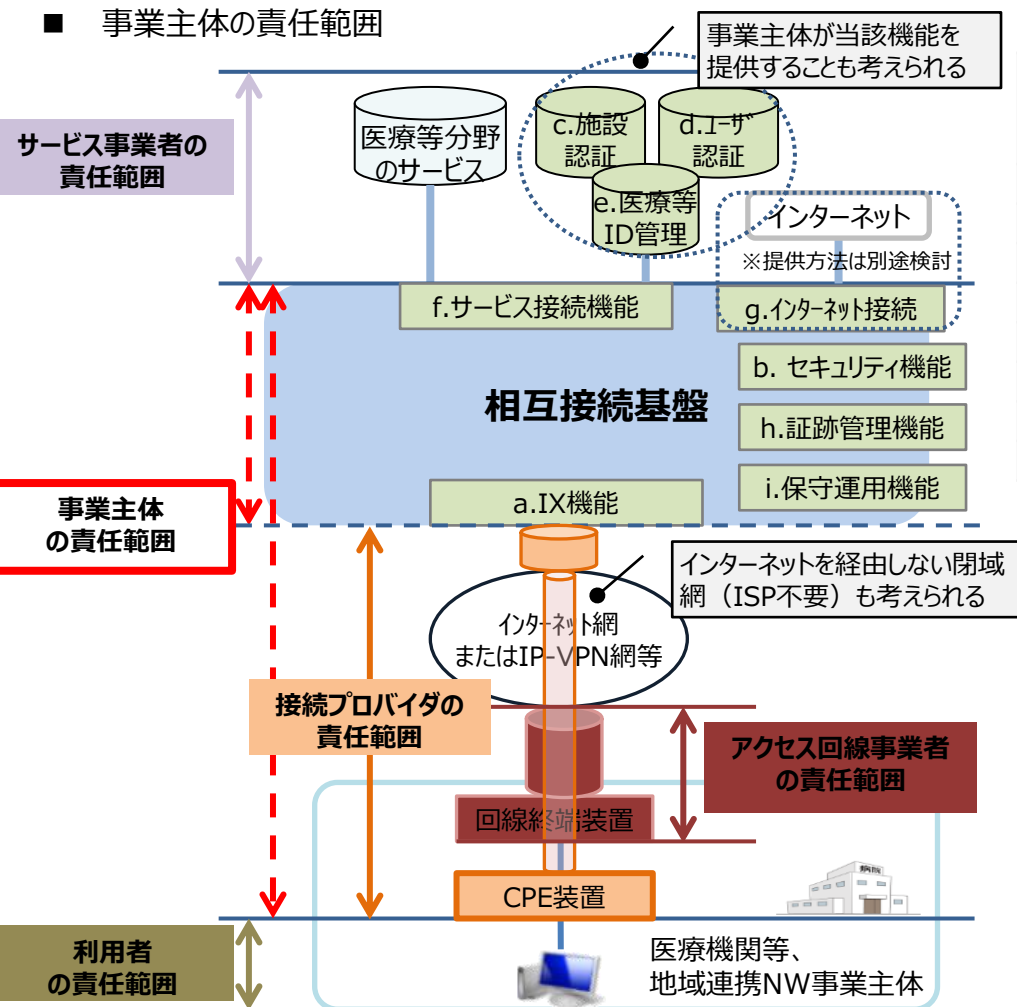
- 相互接続基盤は、今後の医療等分野の様々なICT政策を支える必要不可欠なインフラとして、**患者**や**行政機関**、**医療機関等**、**地域医療情報連携ネットワーク実施主体**など様々なステークホルダーにとって、**様々な便益が期待**。



# 事業主体の責任範囲及び提供機能

- 事業主体の責任範囲は、**相互接続基盤に限定した方式**（利用者との契約は接続プロバイダが担う）と**相互接続基盤までの接続サービスを含める方式**（利用者との契約も基本的に事業主体が担う）の2パターンを想定。
- 各機能の提供主体は異なる可能性はあるが、全ての機能が必須機能であり、そのうち、相互接続基盤の役割を鑑みると、**事業主体は、「a.IX機能」、「b.セキュリティ機能」、「f.サービス接続機能」、「h.証跡管理機能」、「i.保守運用機能」を提供する必要有。**

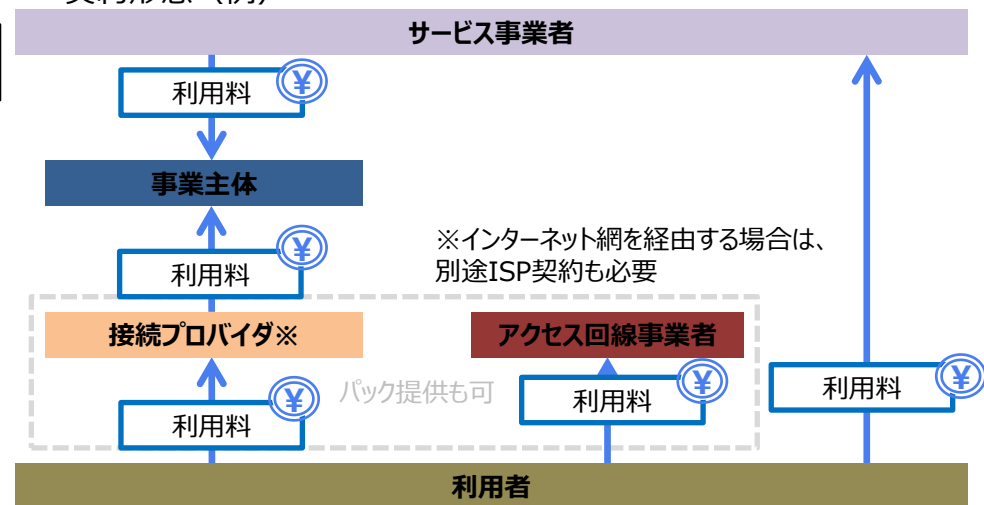
## ■ 事業主体の責任範囲



## ■ 医療等分野で必要な機能及び事業主体による提供必須機能

機能一覧	機能概要	事業主体による提供必須機能
a.IX機能	接続プロバイダの相互接続性を提供	●
b.セキュリティ機能	相互接続基盤のセキュリティ対策	●
c.施設認証機能	医療機関等の施設認証	要検討
d.ユーザ認証機能	医療従事者等の利用者認証	要検討
e.医療等ID管理	医療等IDを管理する機能（発番機能は除く）	要検討
f.サービス接続機能	サービス事業者の接続	●
g.インターネット接続	診療等に必要の限定サイトを接続する機能	要検討
h.証跡管理機能	相互接続基盤の通信ログを取得・管理	●
i.保守運用機能	ヘルプデスク、障害復旧、利用者管理	●

## ■ 契約形態 (例)



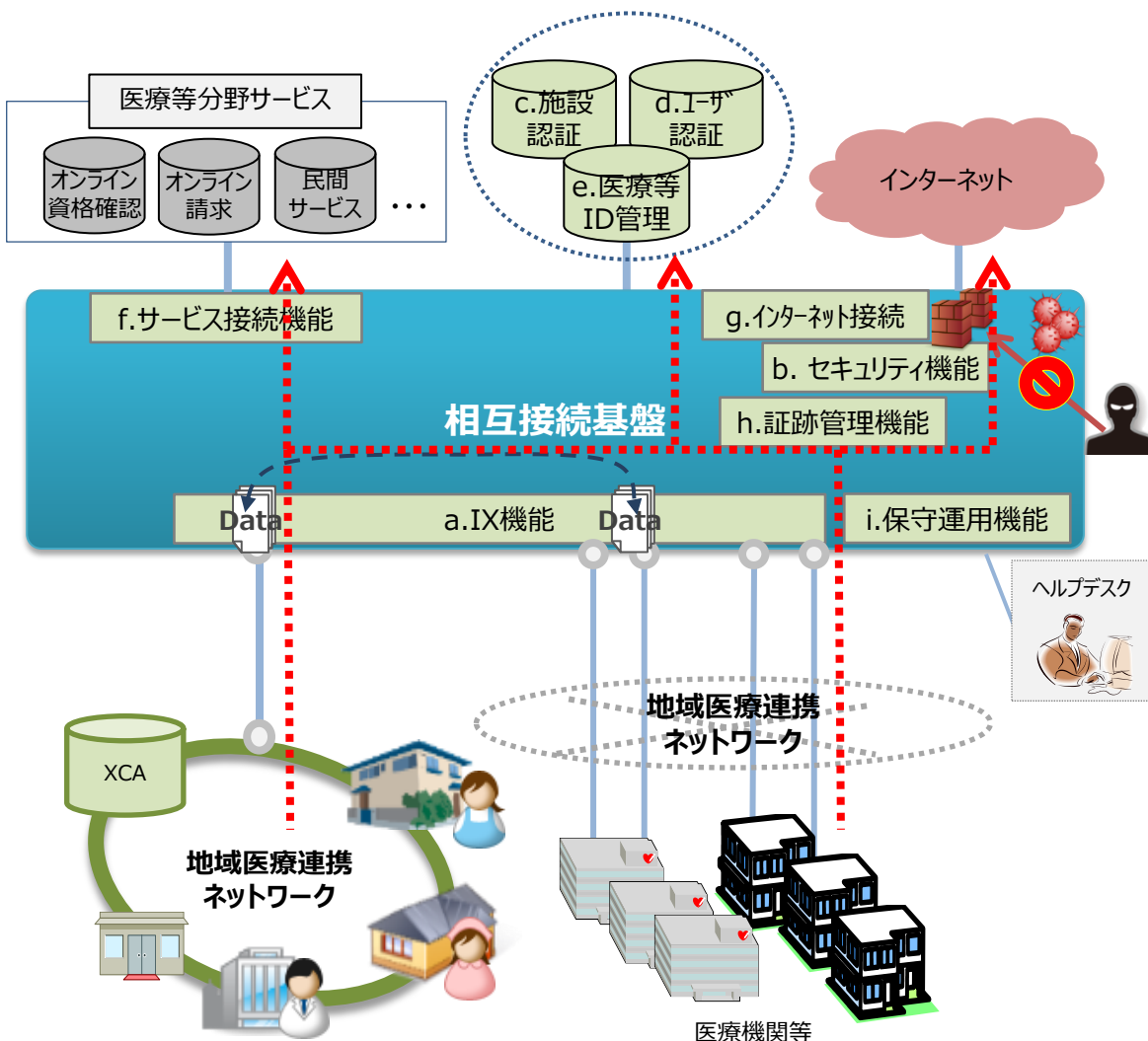


# 參考資料

# 基盤WG検討の全体像 -相互接続基盤設計の考え方-

抽出した9つの機能について、設計・構築し、**実フィールド (A~E) にて検証。**

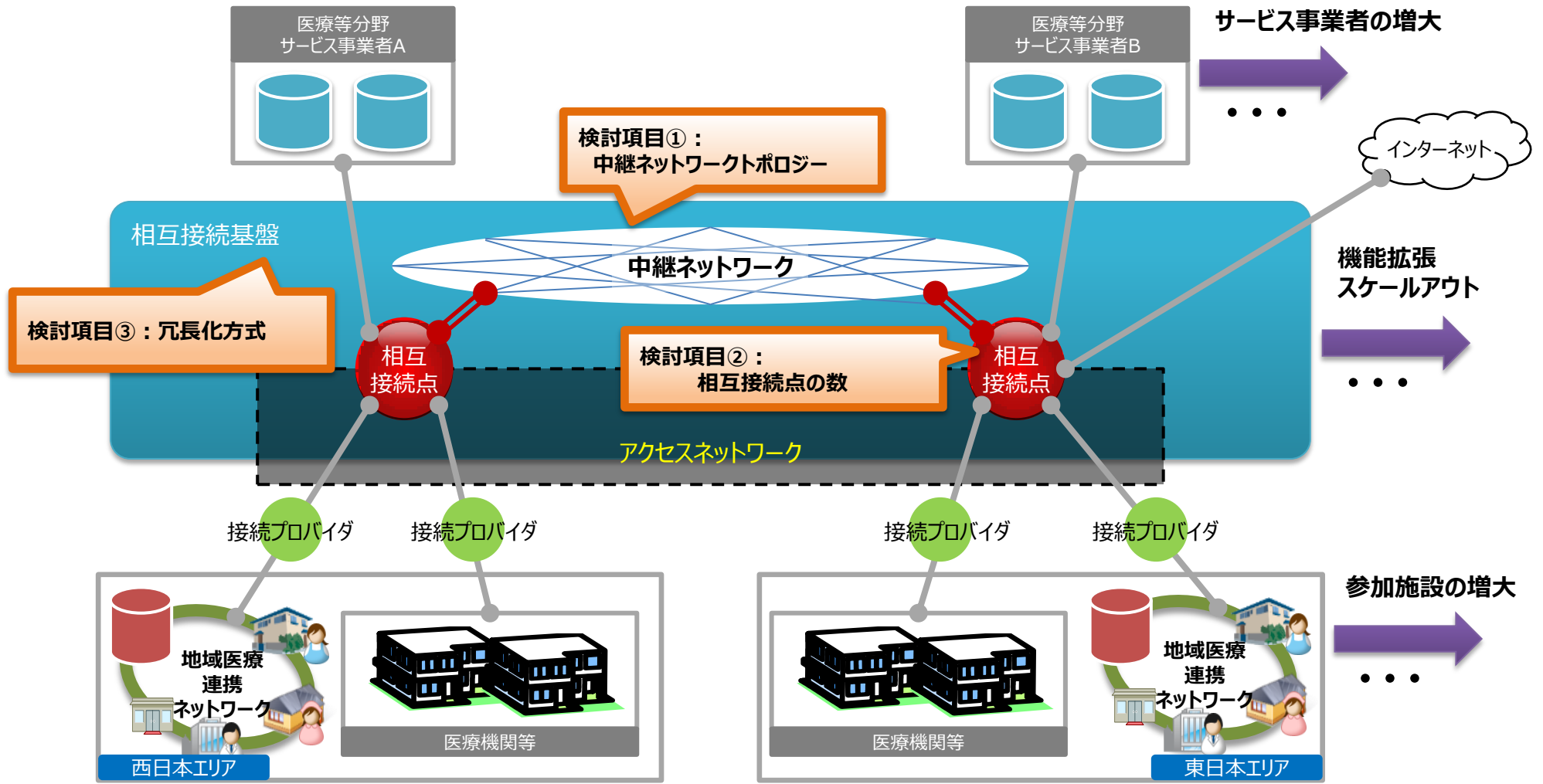
<機能配備図>



機能	フィールド
a. IX機能 接続プロバイダの相互接続性を提供	A B C D E
b. セキュリティ機能 相互接続基盤のセキュリティ対策	A C
c. 施設認証機能 医療機関等の施設認証	B C
d. ユーザ認証機能 医療従事者等の利用者認証	A B C
e. 医療等ID管理 医療等IDを管理する機能	A
f. サービス接続機能 サービス事業者の接続	A B C
g. インターネット接続機能 診療等に必要の限定サイトに接続する機能	C
h. 証跡管理機能 相互接続基盤の通信ログを取得・管理	A B C D E
i. 保守運用機能 ヘルプデスク、障害復旧、利用者管理	A B C D E

# 相互接続基盤全体のアーキテクチャー（概要）

- 相互接続基盤全体のアーキテクチャーは、医療機関等を接続する「**アクセスネットワーク**」と相互接続点間を接続する「**中継ネットワーク**」により構成。
- 相互接続基盤にて流通する**ネットワークトラフィックの効率的配分**、および**セキュリティの確保**、また、参加施設数およびサービス事業者の増大を想定した**柔軟な機能拡張・スケールアウト**に対応。



# 相互接続基盤全体のアーキテクチャー（中継ネットワークトポロジー・相互接続点の数）

- 中継ネットワークトポロジーは、NW断時にも迂回路を複数持つ**メッシュ型**を採用。
- 相互接続点の数は、最小**2拠点**からスタートし、参加施設数に応じた**スケールアウト可能な構成**。

## 検討項目①：中継ネットワークトポロジー

○ 相互接続点    □ あるべき姿    □ 実証構成

	スター型	リング型	メッシュ型 (部分を含む)
イメージ			
特徴	<ul style="list-style-type: none"> <li>中継点間の通信は中心となる中継点を必ず経由するためトラフィック管理が容易</li> <li>中心となる中継点の災害はネットワーク全体に通信影響が及ぶ</li> </ul>	<ul style="list-style-type: none"> <li>2箇所以上の中継点に災害が発生した場合は、通信影響が発生する可能性がある</li> <li>中継点を増設する場合は、どの位置に配置するか検討が必要</li> </ul>	<ul style="list-style-type: none"> <li>中継点の災害が全体に与える影響が最も小さい</li> <li>中継点を増設する場合は、複数中継点とのパスの構築が必要</li> </ul>

## 検討項目②：相互接続点の数

	2拠点 (東京・大阪、札幌・福岡等)	7拠点 (主な主要都市)	47拠点 (各都道府県に1拠点)
イメージ			
特徴	<ul style="list-style-type: none"> <li>相互接続基盤のコストが最小</li> <li>距離で費用変動する専用線の場合は利用者のコスト負担が大きい</li> </ul>	<ul style="list-style-type: none"> <li>医療機関等が多く集まっている都市部に中継点を設けることで、バランスに優れる</li> </ul>	<ul style="list-style-type: none"> <li>相互接続基盤のコストが最大</li> <li>障害発生時の影響範囲が最小</li> <li>距離で費用変動する専用線の場合は利用者のコスト負担が小さい</li> </ul>

- 冗長化方式は、機器故障と災害等の種類の異なるインシデントに対応するため、**機器及び相互接続点冗長を併用**。
- 本実証では、機器冗長は構成せず、スケールアウト可能な検証実施を目的に相互接続点冗長を採用。

## 検討項目③：冗長化方式

■ あるべき姿



■ 実証構成

	機器冗長	相互接続点冗長
イメージ	<p style="text-align: center;">相互接続点</p>	<p style="text-align: center;">相互接続点</p>
概要	システムを構成するネットワーク機器を二重以上で並行運用	システムを構成するネットワーク機器を設置している拠点（相互接続点）を2箇所以上で並行運用
特徴	<ul style="list-style-type: none"> <li>• 機器の故障に対する備え</li> <li>• 故障してから復旧まで1～2日程度要す</li> <li>• 機器のライフサイクルは5～数年</li> </ul>	<ul style="list-style-type: none"> <li>• 地震や洪水などの災害に対する備え</li> <li>• 施設が破壊されると復旧まで数ヶ月以上要す</li> <li>• 施設のライフサイクルは20～数十年</li> <li>• 施設が破壊されると内蔵されている設備も破壊される</li> </ul>

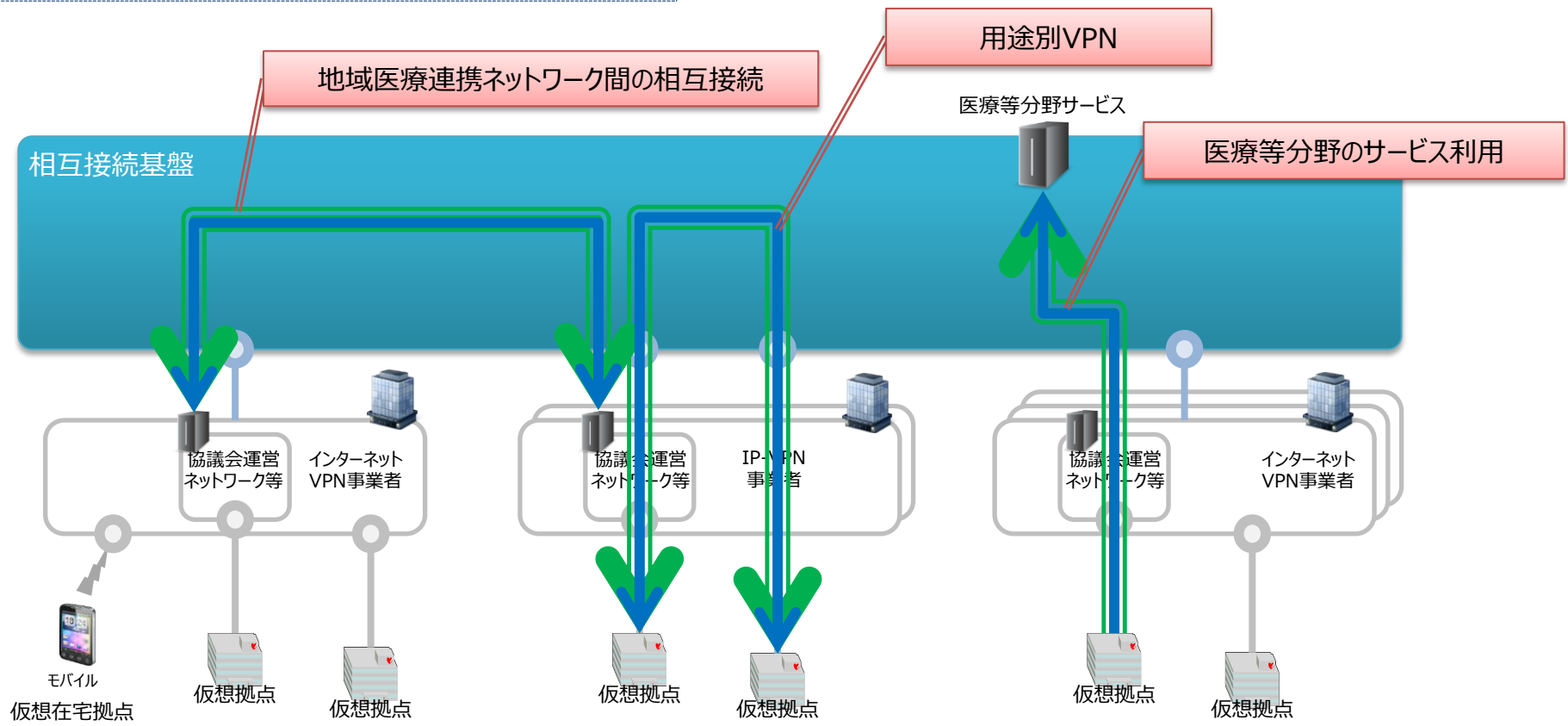
# IX機能の検討（概要）

- 実証に参加した6社の接続プロバイダ※**がサービス提供しているネットワークと同等の実証用環境にて、地域医療連携ネットワーク間の相互接続、医療等分野のサービス利用、用途別VPNのユースケースにおいて、**相互接続基盤経由で通信できることを確認**。  
 ※接続プロバイダ・・・相互接続基盤へのNW接続を提供するVPNサービス提供事業者

凡例

 STEP1（ネットワークレベル）  
 STEP2（アプリケーションレベル）

※図中には、通信例を記載



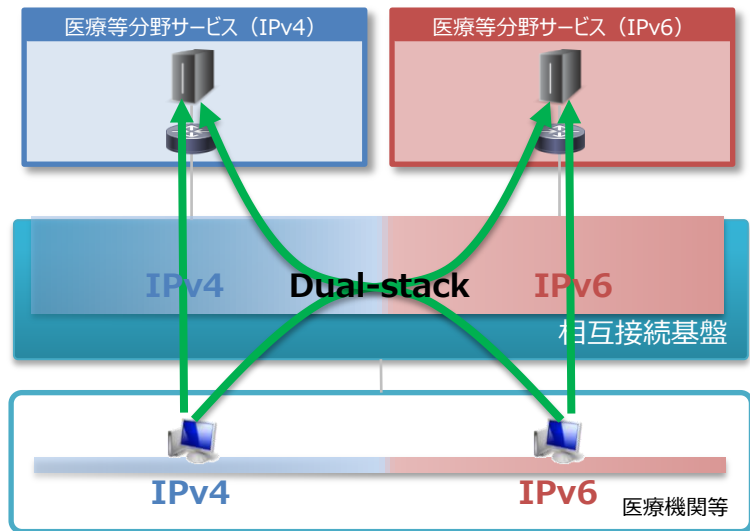
# IX機能の検討（IPアドレス重複回避方法①）

- **相互接続基盤、サービス事業者、医療機関等それぞれのネットワーク**において、IPアドレス方式を**IPv4およびIPv6**とした場合の接続性の確認および課題の洗い出しを実施。
- IPv4通信の場合、IPアドレス重複を回避するために、NAT※に対応した機器の調達、設計構築、運用が必要であり、**運用負担の増大が課題**。 ※NAT…アドレス変換方式

## 検証概要

平成28年度「医療等分野におけるネットワークの相互接続の実現に向けた調査研究」（厚労省）結果から、本実証においては、相互接続基盤をIPv4/IPv6デュアルスタックにて設計。

<IP設計イメージ>



相互接続基盤をIPv4/IPv6デュアルスタック時のケースとして、医療機関等及びサービス事業者（IPv4/v6）を想定し、通信環境を整備し、接続性確認を実施。

- IPv4：シェアードアドレス
- IPv6：グローバルアドレス

## 検証結果

IPv4/v6各ケースにおいて、接続性（IPリーチャビリティ）を確認。

接続パターン	1	2	3	4	5	6	7	8
サービス事業者	IPv4	IPv6	IPv4	IPv6	IPv6	IPv4	IPv6	IPv4
相互接続基盤	IPv4	IPv4	IPv4	IPv4	IPv6	IPv6	IPv6	IPv6
医療機関等	IPv4	IPv4	IPv6	IPv6	IPv6	IPv6	IPv4	IPv4
実証結果	○	○	— (※1)	— (※1)	○	○	○※2	○※2

※1. 医療機関等IPv6、相互接続基盤IPv4、の構成は効果が薄いと考えられるため机上検討  
 ※2. IPリーチャビリティは確認できたが、DNS含めたサービス接続は出来なかった

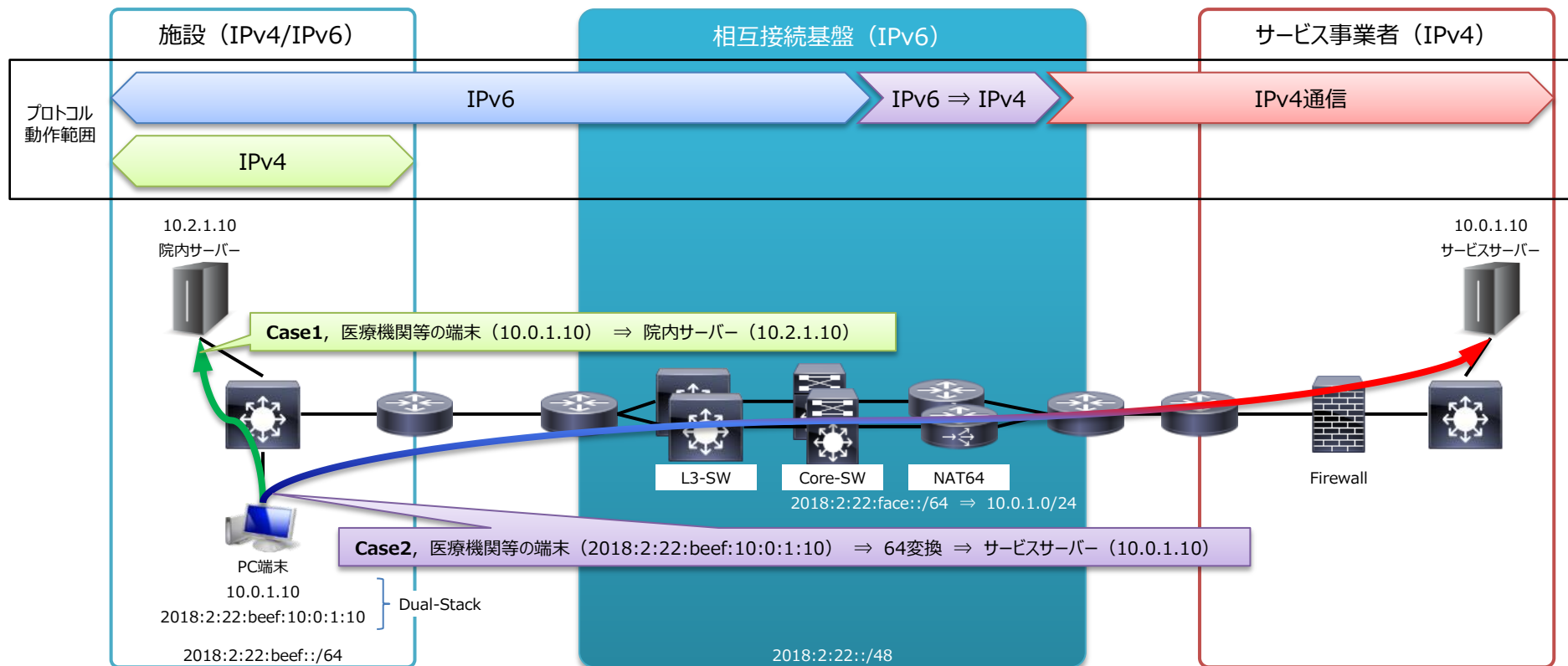
### ■ NATを利用する構成での留意事項

以下の条件を満たし、医療機関等とサービス事業者、相互接続基盤で整合性を保たなければならない。

- 通信元（施設）と通信先（サービス事業者）で使用しているIPアドレス設計を常に把握すること
- 緩衝NWで使用するIPアドレスは通信元と通信先で使用されないことが将来的に保証できること
- 通信元や通信先が増減する都度、変換テーブルの設定変更を行うこと
- サービス事業者のアプリケーションは、NAT環境で使用されることを想定して構築すること
- NAT環境で通信ができないアプリケーションやプロトコルを当該NWでは使用しない規定を準備すること
- NATセッションの枯渇を招かないサイジングを行うこと

# IX機能の検討（IPアドレス重複回避方法②）

- IPアドレス重複の回避方法として、NATを利用しない**IPv6**を採用。
- ただし、サービス事業者については、IPv6に限定するとサービスの制約になることを考慮し、IPv4にも対応。
- なお、医療機関等の施設内については、IPv4およびIPv6の両立が可能であり、既存のIPv4利用も可能。



## <IPアドレス方式>

- 医療機関等とサービス事業者に対して、相互接続基盤上で**一意になるIPv6アドレスを割当て**
- 医療機関等の端末にて**IPv6を有効化**することで、相互接続基盤とIPv6で通信する（IPv4を阻害しない、両立可能）
- 相互接続基盤にサービス事業者向けの**アドレス変換装置を設置**（IPv6⇒IPv4）

## 凡例

- IPv4通信
- IPv6 ~ IPv4通信



# セキュリティ機能の検討①

- 相互接続基盤のセキュリティとして、**外部からの侵入（悪意のある人からの攻撃）**を想定し、必要な機能を検討。
- 攻撃者より情報資産を守るため、通信経路上に**多層防御構造**を取入れ、SOCによる**セキュリティ監視**により、通信に潜む脅威を検知、遮断。

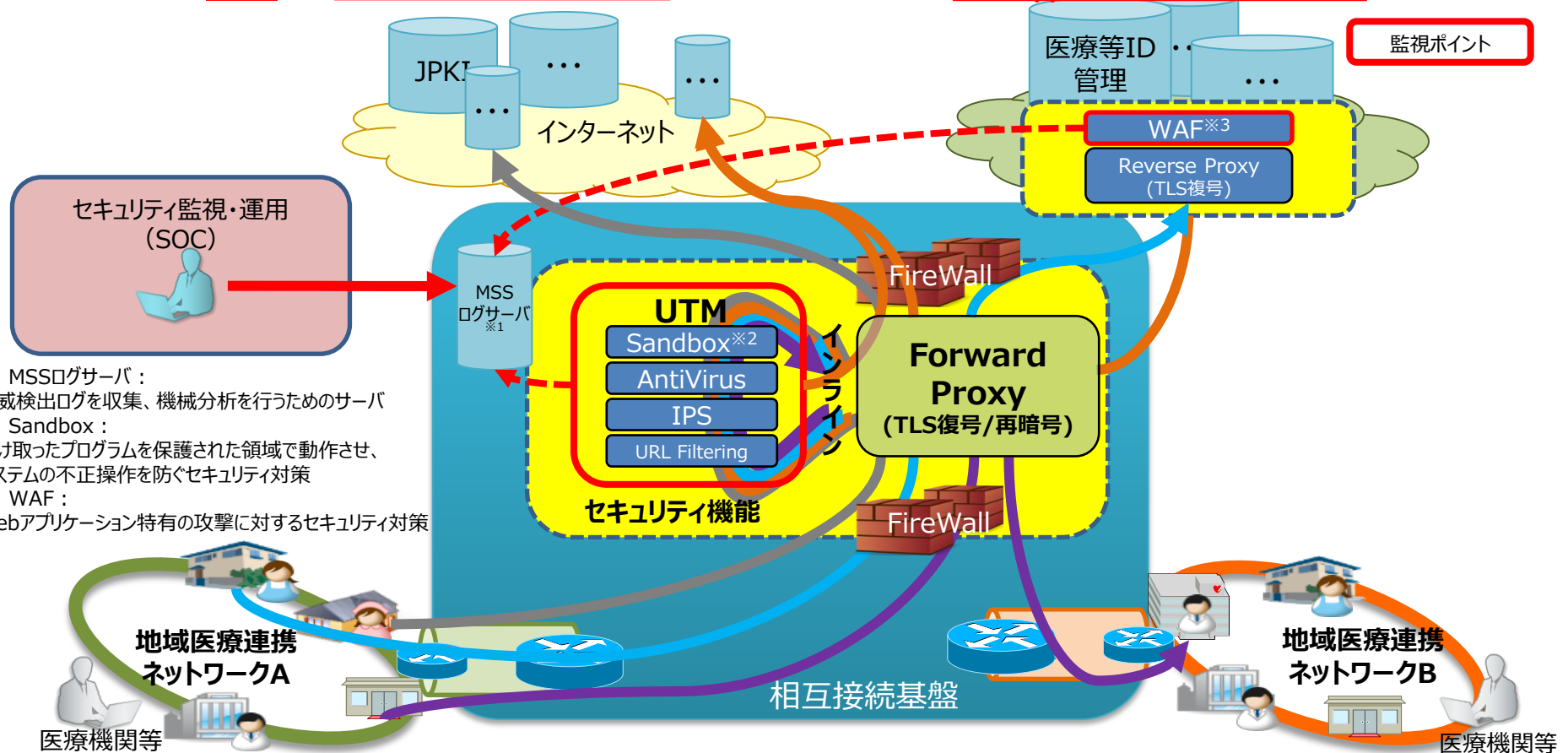
【セキュリティ機能概念図】

インターネット接続

インターネット接続およびインターネット上の医療等分野サービスへの通信を保護するため、**Forward Proxy (TLS復号化/再暗号)** および**IPSやSandbox等を含めたUTM**にて対策

LAN接続・専用接続

上記に加えLANおよび専用接続された医療等分野サービスへの通信を保護するため、**Reverse Proxy (TLS復号化)** および**Web Application Firewall (WAF)**にて対策



- ※1 MSSログサーバ：  
脅威検出ログを収集、機械分析を行うためのサーバ
- ※2 Sandbox：  
受け取ったプログラムを保護された領域で動作させ、システムの不正操作を防ぐセキュリティ対策
- ※3 WAF：  
Webアプリケーション特有の攻撃に対するセキュリティ対策

# セキュリティ機能の検討②

・ **多層防御構造**は、IPS・アンチウイルスによる攻撃・不正トラフィックの検知・遮断、TLS通信の可視化、WAFは有効に機能。URLフィルタリングおよびサンドボックスについては、費用対効果の観点から段階的導入も考慮。SOCによる**セキュリティ監視**は、各フィールドでの通信や模擬通信で、検知・分析・遮断を効率的に実施可能。

## 検証結果

- ・ 多層防御構造 + SOCによる監視運用の結果、インターネット側から多層防御を超えて侵入または攻撃の報告は0件。
- ・ セキュリティ機能の運用で、トラヒック傾向を確認。

### [UTM]

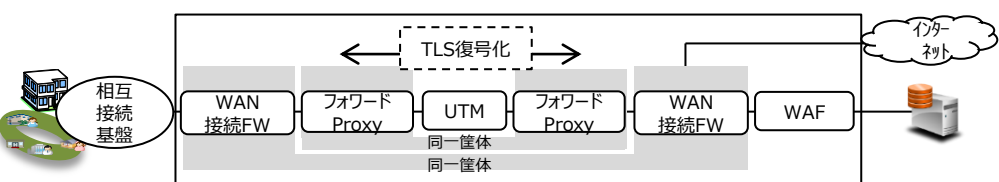
- ・ URLフィルタリング  
インターネット宛のホワイトリスト運用および不要通信遮断において有効。
- ・ IPS・アンチウイルス  
インターネットから相互接続基盤に接続されている端末、APIに対する攻撃・不正トラフィックの検知・遮断において特に有効。
- ・ サンドボックス  
相互接続基盤内部の医療アプリケーションとクライアント間の送受信ファイルに対するセキュリティチェックが特に有効。

### [TLS復号化]

内部通信の9割以上、インターネット通信の4割以上がHTTPS(TLS)であり、UTMでマルウェア検知などのセキュリティチェックを実施する上でTLS復号化は特に有効。

### [WAF]

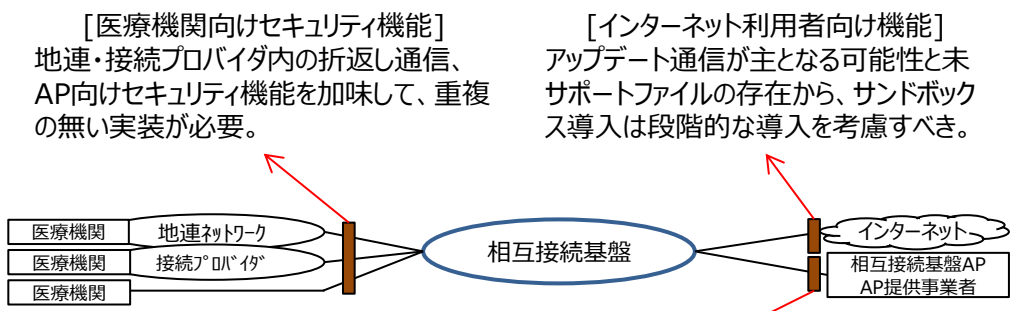
Webアプリケーションの脆弱性を悪用した攻撃の検知・遮断が行われ、Webサーバに対する防御として特に有効。



※WAF (Web Application Firewall) ...Webアプリケーション特有の攻撃に対するセキュリティ対策。

## 考察

- ・ 実用化時は、本実証にて得られた知見を踏まえ、医療機関向け、インターネット利用者向け、AP向けの各セキュリティ機能およびセキュリティ運用を検討、URLフィルタリングおよびサンドボックスは、費用対効果の観点から段階的導入も考慮すべき。

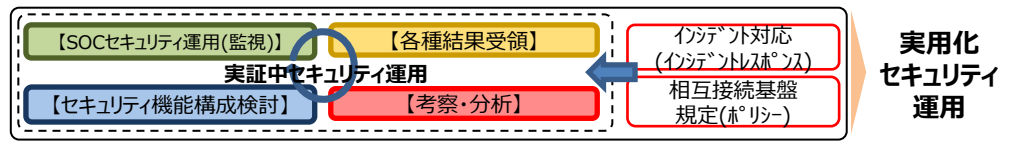


### [API向けセキュリティ機能]

コストの観点からURLフィルタリングは省略または段階的な導入も考慮すべき。

### [セキュリティ運用]

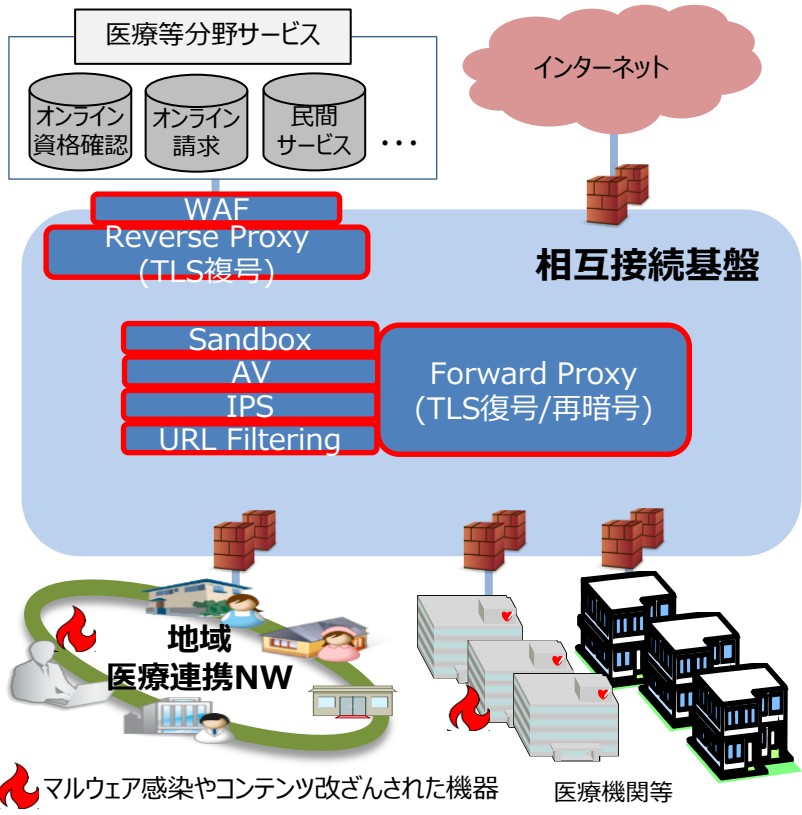
実用化に向けて、運用プロセス・監視および連絡体制を含めたセキュリティ運用の準備と、相互接続基盤規定(ポリシー)を踏まえた、継続的なセキュリティチェックの運用が必要。



# セキュリティ機能の検討③

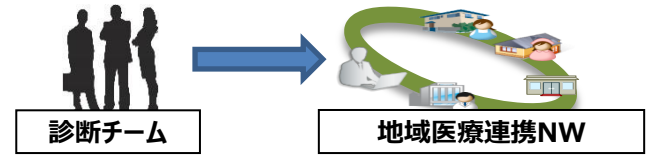
- 相互接続基盤に接続する機関は、医療機関等、サービス事業者、地域医療連携NW等、様々な事業体に跨るため、**各セキュリティ対策のガバナンスの統一**が必要。接続機関によってはセキュリティが十分ではなく、マルウェア感染等も想定される。
- 上記を踏まえ、接続機関に対する**脆弱性診断を行うことによる予防保全**、マルウェア感染等に備え、SOCから提供されるインシデントレポートをもとに、**迅速に被害を最小限に食い止めるプロセス（インシデントレスポンス）の確立が必要**。
- 本実証では、脆弱性診断の有効性およびインシデントレスポンスは、IPAのガイドをもとに、発生源を特定するプロセスを作成・検証。

相互接続基盤の接続は様々な事業体に跨るため  
セキュリティ対策のガバナンスが必要



脆弱性診断による予防保全  
有事の際のインシデントレスポンスが求められる

### 検証1.脆弱性診断の有効性



### 検証2.インシデントレスポンス

#### 検証ユースケース

- 許可サイトにおける水呑場攻撃により医療機関が汚染
- 既に汚染された医療機関からの医療分野サービスへの攻撃
- XCAを使ったマルウェア拡散
- 既に汚染された医療分野サービスから悪性サイトへの誘導



# セキュリティ機能の検討④

- 脆弱性診断については、相互接続基盤への接続前に、**実際に脆弱性を発見し、対処**したことで**予防保全につながった**。接続機関に対する「脆弱性診断サービス」の提供は有効。
- インシデントレスポンスについては、**すべての検証ユースケース**に対し、**通信ログより脅威の発生源を特定**。一方でNATやDHCPを用いたNWでは、IPアドレスの特定に時間を要するため、**IPv6の導入が有効**。XCA間の通信ではXMLファイルの一部のタグが暗号化されており、マルウェア検知が困難であることから、医療機関からのデータアップロード時にマルウェア検知が必要。

観点	課題	考察・対応策
脆弱性診断	<b>接続機関の脆弱性起因によるインシデント</b> <ul style="list-style-type: none"> <li>他接続機関を巻き込んだインシデント事故の誘発。</li> </ul>	<ul style="list-style-type: none"> <li>■ 技術面：Web改ざん検知ソフトウェアの導入や遠隔サービスの適用。</li> <li>■ 運用面：接続にあたっての事前診断や定期診断の実施。ただし、相互接続基盤が受益者負担型のセルフリモート診断サービスを提供する運用も考慮。</li> <li>■ 制度面：相互接続基盤への接続にあたってのガイドライン策定。</li> </ul>
インシデントレスポンス	<b>NATやDHCPを用いたNW構成による運用の煩雑化</b> <ul style="list-style-type: none"> <li>各NW機器のログを突合する必要があり、脅威の発生源の特定に時間を要する。</li> </ul>	<ul style="list-style-type: none"> <li>■ 技術面：IPv6導入によるNATを用いないNW設計。ただし、対応機器の選定やツールによる可読性の向上等、更なる煩雑化を招かないよう考慮する必要あり。</li> <li>■ 運用面：適切なチーム構成と迅速な意思決定を行うセキュリティ責任者を各事業者に配置。</li> <li>■ 制度面：接続機関への情報の提供。（NATログが出力される機器等）</li> </ul>
	<b>XCAを用いた地連間の通信における脅威の未検知</b> <ul style="list-style-type: none"> <li>XCA-GW間の通信においては、ファイル内の一部のデータがBASE64でエンコードされており検疫が困難。</li> </ul>	<ul style="list-style-type: none"> <li>■ 技術面：対象となるメッセージ部分のみ抜粋、アプリケーションレイヤでの対応。（iRule等）</li> <li>■ 運用面：XCAに係るサーバを相互接続基盤内にホスティングし、ファイル配置時にセキュリティ機能による検疫。</li> <li>■ 制度面：接続機関へのルール化。</li> </ul>
	<b>個人情報を含むログに対する漏えいリスク</b> <ul style="list-style-type: none"> <li>情報漏えい事故への懸念。</li> </ul>	<ul style="list-style-type: none"> <li>■ 技術面：サンドボックスへの検体の場合、exeファイル等、対象とする検体の絞り込みを行うことや、利用するサンドボックスの事業者がSOC2認定等を取得しているか確認。</li> <li>■ 運用面：閲覧や調査で知り得た情報の取り扱いに関する制限。</li> <li>■ 制度面：運用ルールの厳格化。（作業者の同意等）</li> </ul>

# 施設認証機能の検討①

施設（医療機関等）から申請、相互接続基盤事業主体等が認定後、認証キーとして**電子証明書**を**ネットワークレイヤー（L3）、アプリケーションレイヤー（L4以上）**の2種類の電子証明書を発行し、ルーター、端末に用いて検証。

## 検証構成（概要）

### ■ 施設認証の目的

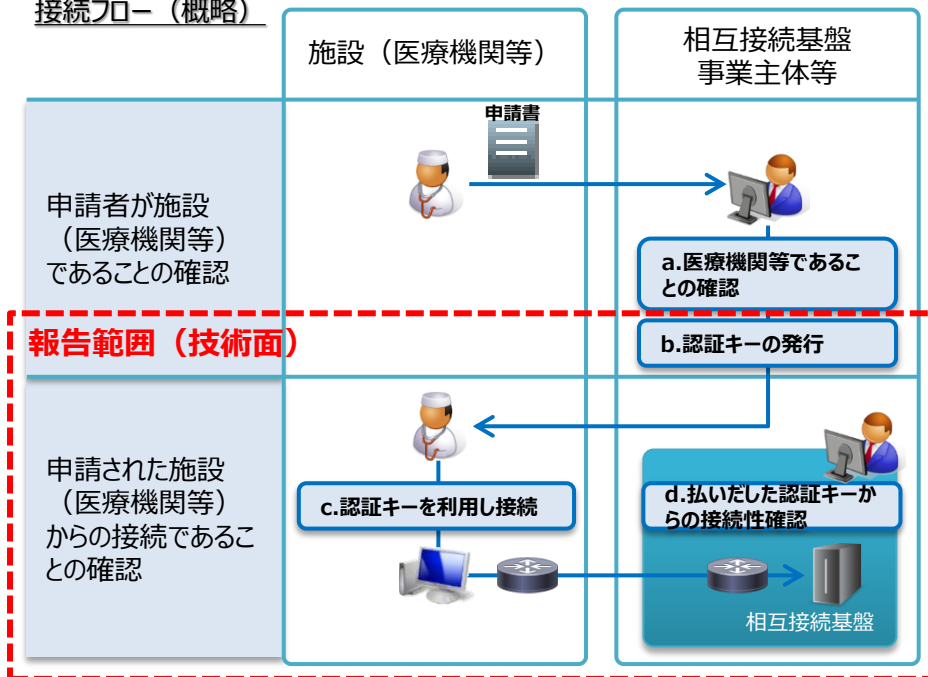
相互接続基盤に接続する施設を認証（医療機関等に絞る）、確実に接続を行うこと。

### ■ 施設認証の手段

施設認証を行うにあたり、以下の接続フローを想定。

- 申請者が医療機関等であることの確認
- 申請された医療機関等からの接続であることの確認

### 接続フロー（概略）



## 検証計画

### ■ b. 認証キーの発行

相互接続基盤に接続する際に、技術的に施設を識別する方法として以下2つを検討。

#### ・ ネットワークレイヤーで認証を行う方法

施設側ルーターでIPsecを用いる際の**認証キー**として**電子証明書と比較のため共有鍵（Pre-Shared Key）**を用いて検証。

#### ・ アプリケーションレイヤーで認証を行う方法

施設側PCで認証キーとして**電子証明書\***を用いて検証。

→ 本実証では共通的に利用できる**電子証明書（施設別）**を用いた**施設認証キー**を利用。 ※HPKIにて発行される電子証明書を利用。

### ■ c. 認証キーを利用し接続 / d. 払いだした認証キーからの接続性確認

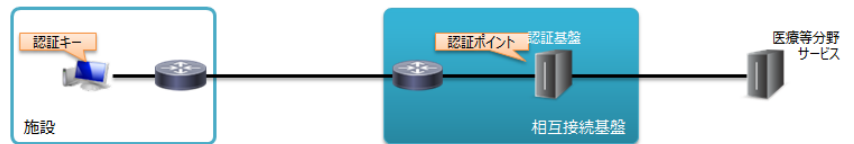
#### ・ ネットワークレイヤーで認証を行う方法

全国規模でのネットワークを想定し、同一メーカーではなく複数のメーカーのルーターを準備して**同一メーカー同士、異なるメーカー同士にて検証**



#### ・ アプリケーションレイヤーで認証を行う方法

認証基盤（統合ポータル）で電子証明書を用いたクライアント認証にて検証



# 施設認証機能の検討②

- 認証キーとして電子証明書を採用する場合、その適用範囲は、**アプリケーションレイヤー（L4以上）**が有効。
- ネットワークレイヤー（L3）の認証については、施設（医療機関等）の接続回線、利用用途に応じて、Pre-shared key※等、**幅広い認証方式**が望ましい。 ※通信を暗号化する際の事前共有鍵

## 検証結果

### ネットワークレイヤーで認証

ルーターベンダ別検証表

説明凡例 ○：接続成功、×：接続不可、-：重複項目のためスキップ  
 証明書（HPKI）：HPKIより発行  
 証明書（自己署名）：RFC4945に準拠し独自に発行

RFC実装	RFC実装	認証方式	A社	B社	C社	D社
			RFC4945	RFC4306	RFC4945	非公開
A社	RFC4945	証明書（HPKI）	×	-	-	-
		証明書（自己署名）	○	-	-	-
		共有鍵（パスワード）	○	-	-	-
B社	RFC4306	証明書（HPKI）	×	×	-	-
		証明書（自己署名）	○	○	-	-
		共有鍵（パスワード）	○	○	-	-
C社	RFC4945	証明書（HPKI）	×	×	○	-
		証明書（自己署名）	○	×	○	-
		共有鍵（パスワード）	○	○	○	-
D社	非公開	証明書（HPKI）	機能なし	機能なし	機能なし	機能なし
		証明書（自己署名）	機能なし	機能なし	機能なし	機能なし
		共有鍵（パスワード）	○	○	○	○

※RFC4945・・・IPsec+IKEv2に電子証明書を用いる場合の電子証明書の発行仕様を規定  
 ※RFC4306・・・IPsec+IKEv2に電子証明書を用いてもよいことを規定（現在は廃止）

#### ■ HPKIの電子証明書利用による分類

本来ルーターでの利用を想定していないHPKIの電子証明書（ISO17090に準拠）を使用したため、**C社同士の除外多数のパターンにおいて接続に失敗**したと考えられる。

#### ■ RFC実装の違いによる分類

異なるRFCを採用しているA社とB社のルーター間で接続に**成功**したこと、B社とC社のルーター間で接続に**失敗**したこと、同じRFC4945を採用しているA社とC社のルーター間で接続に**失敗**したことについてメーカー問い合わせを行ったところ、**RFC4945は証明書の発行仕様であり、ルーターの認証機能の実装仕様ではないため、メーカーによって認証機能の実装仕様が異なる**。よって、RFCの準拠は必ずしも接続に成功する根拠や保証とはならないとの回答あり。

#### ■ パスワード（Pre-Shared Key）による認証はいずれの組み合わせでも**成功**。

本実証において、HPKIの電子証明書を使用してネットワークレイヤーの電子証明書認証を行ったが、**多数の組み合わせで認証に失敗する結果が発生**

## 検証結果

### アプリケーションレイヤーで認証

端末OS	結果	利用ブラウザ
Windows 7	○	Internet Explorer 11
Windows 10	○	Internet Explorer 11

- 相互接続基盤の認証基盤は電子証明書の特定の属性項目を参照し、その値によって異なる処理を実行可能。
- HPKIで発行する電子証明書に施設単位で一意的な識別番号を予め付与しておき、端末に導入。
- 認証基盤で端末を認証する際、この識別番号を参照して異なる医療等分野のサービスを表示することが可能。

## 課題・考察

課題	考察
電子証明書の適用範囲をL3とした場合、同一メーカー同士であっても、認証に失敗する結果が発生	証明書を変更することにより、成功する事例が増えたものの、ルーターの認証機能の実装差異があるため、構築可能な機器が限定されてしまう。 ネットワークレイヤーの認証には、電子証明書を使用せず、回線認証、Pre-Shared Key等を用いた認証を検討すべきである。 また、電子証明書を使用して接続できるルーターを、事業主体が認定する方法も考えられる。

# ユーザー認証機能の検討①

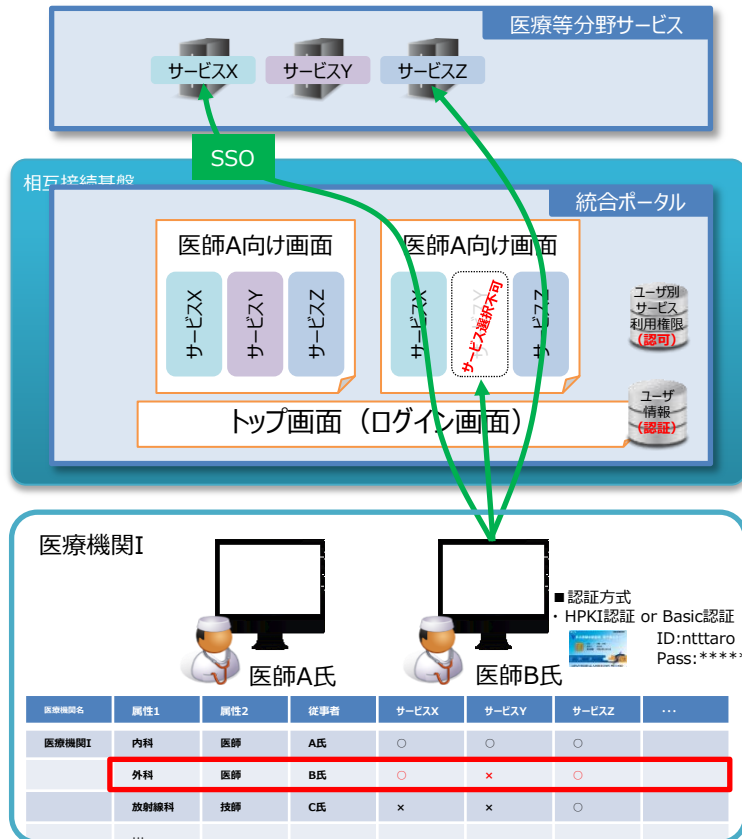
- 医療機関の医師等をユーザー認証し、**ユーザー毎に利用可能な機能や情報を認可（利用権限）**する環境を構築、**「ユーザー認証方式」、「複数サービスの集約」、「外部サービスとの連携」**の3つの観点で検証。

## 検証構成（概要）

### ■ ユーザー認証の目的

医療機関の医師等を**認証**し、ユーザー単位にサービスの利用を**認可（利用権限）**すること

ユーザー認証概要図（統合ポータルを利用）



## 検証計画

### ■ フィールドごとの実証環境条件

凡例 ○：実装あり、△：一部実装、×：実装なし

フィールド	ユーザー認証方式	複数サービスの集約	外部サービスとの連携
A (岡山、島根、香川)	○ Basic	×	×
B (前橋、酒田)	○ HPKI	○	○
C (沖縄)	○ HPKI /Basic	△	×

### ■ 検証内容

【観点①】ユーザー認証方式

- ・HPKI or Basic (ID/Password)

【観点②】複数サービスの認証機能の集約

- ・統合ポータル
- ・シングルサインオン (SSO)

【観点③】外部サービスとの連携

- ・医療等分野サービスとの連携

# ユーザー認証機能の検討③

- ユーザー認証の機能としては、複数のユーザー認証方式（HPKI/Basic）の対応、統合ポータルによる認証機能の集約、外部サービスとの連携が**利便性の面で有効**。

## 検証結果

## 課題・考察

観点	フィールド	インタビュー結果
①複数の認証方式	A (岡山、島根、香川)	<ul style="list-style-type: none"> <li>ユーザー認証は、現状、医療機関任せとなっている。HPKI認証でも、その先生がどの施設に所属しているかの情報が無い。<b>相互接続基盤の接続先から、誰がどの組織としてアクセスしてきたかわからない。</b></li> </ul>
②複数サービスの集約	B (前橋、酒田)	<ul style="list-style-type: none"> <li>必要な画像情報に早くたどり着くことが必要であり、<b>操作性の改善</b>が必要。</li> </ul>
	C (沖縄)	<ul style="list-style-type: none"> <li>HPKIカードで認証して統合ポータルにログインできても、統合ポータルからアプリにログインする際に別途認証が必要となる。HPKIのカードを何度もかざすのはわずらわしい。<b>SSOを利用した方が便利</b>である。</li> </ul>
③外部サービスとの連携	B (前橋、酒田)	<ul style="list-style-type: none"> <li>HPKIのログイン時間が遅いの気になる。<b>早く診療情報を取得・参照できることが医療現場として重要な要素</b>であると言える。</li> </ul>

	課題	考察
①旧OSでの処理時間によるストレス	<ul style="list-style-type: none"> <li>画面遷移のパフォーマンス計測により<b>処理時間で大半を占めるのはHPKIカードの読み込み</b>と判明。</li> <li>HPKIカードの読み込みはカードRWを制御するOS依存の処理であるため、<b>旧OS (Windows 7) に処理時間の遅さが顕著</b>。</li> </ul>	<ul style="list-style-type: none"> <li>医療等分野サービスのサポートOSは<b>Microsoftを原則とし、新OSへの移行推進・啓蒙</b>が必要。現場の医療従事者等の<b>利用時にストレスを与えない方式の実装</b>も必要。</li> <li>旧OSは医療等分野サービスがサポートしても、外部認証サービスがサポートしないケースもある。医療等分野サービスでは<b>OSに応じた認証方式の検討や、採用した認証方式の認証レベルに応じた認可の制御</b>も必要。</li> </ul>
②複数サービスの証明書をダイアログで選択する手間と処理時間	<ul style="list-style-type: none"> <li>受診履歴管理サービスとJPKI署名検証PFサービス（PINなし認証）とで<b>異なる2つ（複数）のクライアント証明書</b>を必要とするため、各サービスの利用時に必ず証明書の選択ダイアログが表示される（仕様上、不可避）。</li> <li>目的のサービスのクライアント証明書を<b>選択する操作に手間と時間を要する</b>。誤選択時のエラー対処もわかりにくい。</li> </ul>	<ul style="list-style-type: none"> <li>医療等分野サービスで<b>共通のクライアント証明書（相互接続基盤の指定認証局が一元管理・提供）</b>を使用し、証明書の選択ダイアログの表示を回避することが望ましい。</li> </ul>
③HPKI認証とJPKI署名でカードRWを共用できない	<ul style="list-style-type: none"> <li>受診履歴管理サービスでは同一端末、同一ブラウザでの一連の操作でHPKI認証とJPKI署名を行う想定だった。</li> <li>しかし、<b>同一端末上でHPKIドライバとJPKIドライバにカードRWの競合が発生</b>し、後続のJPKI署名が行えなかったため、2つのカードRWを個別に割り当てたことで対処。</li> <li>HPKI認証とJPKI署名で<b>カードRWを使い分けざるを得ない</b>。（カードRWの共用 or 分離を選択不可）</li> </ul>	<ul style="list-style-type: none"> <li>外部サービスが提供するクライアントアプリケーション（例えば、HPKIドライバ等）は、必ずしも同一端末上で他のアプリケーションとの共存を想定した実装とは限らない。</li> <li>相互接続基盤の運営主体は、<b>外部サービスと連携するためのガイドラインやテスト環境を提供し、事前検証を推奨</b>することが必要。</li> </ul>



# ユースケース/ステークホルダー

- ステークホルダーは、相互接続基盤へ接続することが想定される **医療機関等、サービス事業者、地域医療連携ネットワーク運営主体** 以外に、ユースケースが実現されることによって便益が見込まれる **患者、行政機関、医療システム事業者・医療機器事業者、情報収集機関** の大きく7つに分類。また、17のユースケースを整理。

ユースケース	ステークホルダー						
	医療機関等 (病院、医科・歯科診療所、薬局、介護施設等)	サービス事業者	地域医療連携ネットワーク運営主体	患者	行政機関 (公的サービス提供者等を含む)	医療システム事業者・医療機器事業者	情報収集機関 (行政機関、研究機関、認定事業者等)
① 地域医療連携ネットワーク間連携	●	●	●	●			
② HPKI認証	●	●	●				
③ 医療等IDの利用	●				●		
④ レセプトオンライン請求	●				●		
⑤ オンライン資格確認	●				●		
⑥ 電子紹介状	●	●		●			
⑦ 電子処方箋	●	●		●			
⑧ セキュアメール	●	●					
⑨ 地域医療介護連携 (クラウドを利用した共同利用)	●	●	●	●			
⑩ 遠隔診断支援	●	●					
⑪ 災害・救急時における 医療情報等の活用	●	●				●	
⑫ インターネット接続 (文献検索等)	●	●					
⑬ 医療等情報データベース	●						●
⑭ 医療等情報の二次利用・分析	●						●
⑮ EHR・PHR連携	●	●		●			
⑯ リモートメンテナンス	●	●				●	
⑰ 民間クラウドサービス	●	●					

# 相互接続基盤の利用が想定される施設数

- ユースケースを踏まえ、具体的利用シーンをもとに、医療等分野のサービス普及率の推計し、**利用規模を試算**。

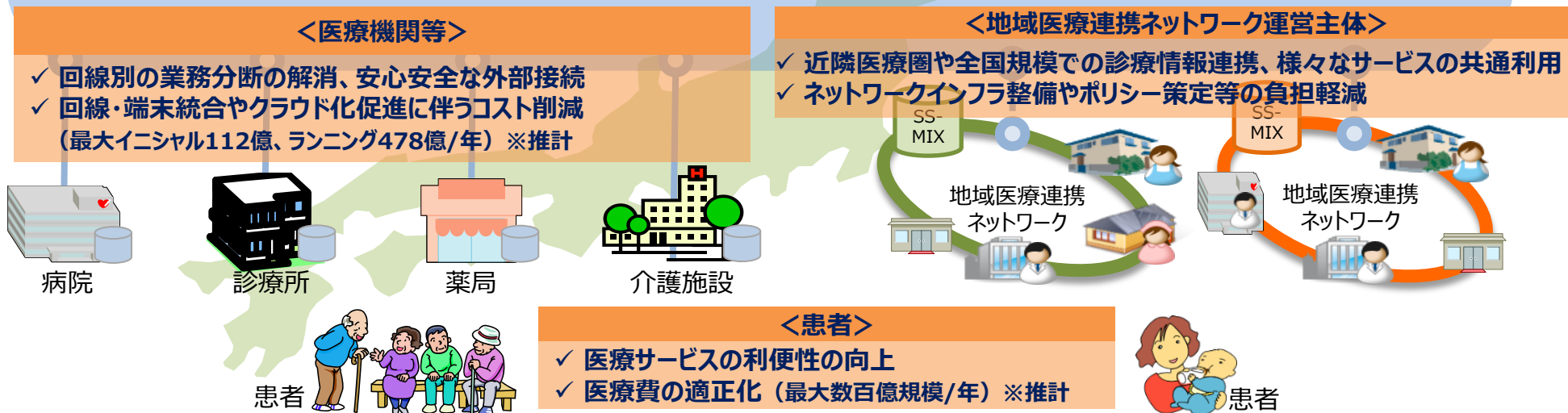
利用シーン	平成32年度の各サービス普及率を推計し試算	平成37年度の各サービス普及率を推計し試算	最大規模
【利用シーン（1）】 地域医療連携ネットワーク間で診療情報を相互参照する場合	【地域医療連携ネットワーク数】 ・ 253箇所	【地域医療連携ネットワーク数】 ・ 253箇所	【地域医療連携ネットワーク数】 ・ 253箇所
【利用シーン（2）】 医療等IDを利用し、地域医療連携ネットワーク内の施設と加入していない施設が医療情報連携サービス（クラウドサービス）を介して、診療情報を相互参照する場合	【地域医療連携ネットワーク数】 ・ 253箇所 【地域医療連携NW未参加施設数】 ・ 134,492施設 ※病院：5,658、医科診療所：62,684、歯科診療所：12,577、薬局：53,573	【地域医療連携ネットワーク数】 ・ 253箇所 【地域医療連携NW未参加施設数】 ・ 149,585施設 ※病院：5,658、医科診療所：73,698、歯科診療所：16,656、薬局：53,573	【地域医療連携ネットワーク数】 ・ 253箇所 【地域医療連携NW未参加施設数】 ・ 221,230施設 ※病院：5,894、医科診療所：91,778、歯科診療所：67,984、薬局：55,574
【利用シーン（3）】 施設間でファイル交換サービス（クラウドサービス）、HPKIによる電子署名を利用して、電子紹介状を連携する場合	【施設数】 ・ 32,869施設 ※病院：3,004、医科診療所：25,767、歯科診療所：1,321、薬局：2,778	【施設数】 ・ 162,357施設 ※病院：8,098、医科診療所：81,672、歯科診療所：16,883、薬局：55,704	【施設数】 ・ 236,840施設 ※病院：8,435、医科診療所：101,709、歯科診療所：68,912、薬局：57,784
【利用シーン（4）】 各施設がレセプトオンライン請求を利用する場合	【施設数】 ・ 146,017施設 ※病院：8,098、医科診療所：69,467、歯科診療所：12,749、薬局：55,704	【施設数】 ・ 162,357施設 ※病院：8,098、医科診療所：81,672、歯科診療所：16,883、薬局：55,704	【施設数】 ・ 236,840施設
【利用シーン（5）】 各施設が医療保険のオンライン資格確認を利用する場合	【施設数】 ・ 146,017施設	【施設数】 ・ 162,357施設	【施設数】 ・ 236,840施設
【利用シーン（6）】 医療機関や医科診療所が電子処方せんサービス、HPKI電子署名を利用して、電子処方せんを薬局と連携する場合	【施設数】 ・ 32,869 施設	【施設数】 ・ 162,357施設	【施設数】 ・ 236,840施設
【利用シーン（7）】 各施設がセキュアメールやインターネット接続を利用する場合	【施設数】 ・ 146,017施設	【施設数】 ・ 162,357施設	【施設数】 ・ 236,840施設
【利用シーン（8）】 依頼医療機関からの放射線画像、病理画像診断依頼に対して、支援医療機関にて遠隔診断支援を実施する場合	遠隔画像診断 【施設数】 ・ 3,114施設 ※病院1,725、医科診療所1,389	【施設数】 ・ 4,066施設 ※病院2,105、医科診療所1,960	※遠隔画像診断を依頼及び支援する最大施設数を想定できないため、試算対象外
	遠隔病理診断 【施設数】 ・ 892施設 ※病院267、医科診療所 625	【施設数】 ・ 1,214施設 ※病院316、医科診療所 898	※遠隔病理診断を依頼及び支援する最大施設数を想定できないため、試算対象外
【利用シーン（9）】 各施設が医療等情報を外部データセンターへバックアップする場合	【施設数】 ・ 74,274施設 ※病院：3,134、医科診療所：25,911、歯科診療所：8,019、薬局：37,210	【施設数】 ・ 99,765施設 ※病院：4,097、医科診療所：38,794、歯科診療所：13,034、薬局：43,839	【施設数】 ・ 236,840施設
【利用シーン（10）】 公的データベースの情報収集、医療等情報の二次利用・分析等ができるように各施設から医療等情報を収集する場合	【施設数】 ・ 74,274施設	【施設数】 ・ 99,765施設	【施設数】 ・ 236,840施設
【利用シーン（11）】 各施設がクラウド型レセプトコンピュータを利用する場合	【施設数】 ・ 35,877施設 ※病院：1,109、医科診療所：11,115、歯科診療所：2,040施設、薬局：21,613	【施設数】 ・ 71,954施設 ※病院：2,773、医科診療所：34,711、歯科診療所：7,175施設、薬局：27,295	【施設数】 ・ 234,241施設 ※病院：5,836、医科診療所：101,709、歯科診療所：68,912、薬局57,784

# ステークホルダー別の導入効果①

- 相互接続基盤は、今後の医療等分野の様々なICT政策を支える必要不可欠なインフラとして、**患者**や**行政機関**、**医療機関等**、**地域医療連携ネットワーク運営主体**など様々なステークホルダーにとって、**様々な便益が期待**。



## 相互接続基盤



# ステークホルダー別の導入効果②

ステークホルダー	導入効果	概要
医療機関等 (病院、医科・歯科 診療所、薬局、介 護施設等)	①安心安全な医療情報共有・ 連携による診療業務の効率化	安心して院外と接続できる環境が整備されることにより、様々な医療等分野のサービスを利用でき、診療業務が一連で行えるようになる。
	②回線統合・クラウド化促進に 伴うICTコスト・管理の最適化	用途別に回線や端末を準備することが不要になり、外部ASP型サービスの利用が促進され、ICT環境の整備や管理に関する費用や業務負荷が軽減される。
地域医療連携 ネットワーク 運営主体	③参加医療機関の加入促進	院外接続におけるセキュリティ障壁が緩和され、地域医療連携ネットワークへの参加がしやすくなる。
	④地域医療連携NWにかかる ICTコスト・管理の最適化	相互接続するためにネットワークを個別に整備することが不要になり、クラウドでの共同利用が促進され、運用費の最適化につながる。
患者	⑤医療サービスの利便性の向上	診療情報連携の促進により、医療サービスの地域格差が是正され、患者が全国どこにいても適切かつ効率的な医療サービスが受けられるようになる。
	⑥医療費の適正化	診療情報連携の促進により重複検査・処方等が削減され、医療費の適正化・患者負担の軽減につながる。
行政機関 (公的サービス事業 者含む)	⑦医療等ICT政策の推進	各施設が個別にネットワークを整備することが不要になるため、様々な医療ICT政策が推進される。
サービス事業者	⑧ビジネス機会の創出	相互接続基盤を利用する施設に対してサービスを提供できるようになり、商機創出・ビジネス拡大につながる。
医療システム事業者・ 医療機器事業者	⑨保守業務の効率化	セキュアなネットワーク上でのリモートメンテナンスが可能になり、現地訪問の稼働削減による保守業務の効率化につながる。
情報収集機関 (行政機関、研究 機関、認定事業者 等)	⑩医療情報の悉皆性の担保 二次利用の促進	収集専用のネットワーク化が不要になり、認定事業者が医療情報の効率的な収集や分析が可能になる。
	⑪公的データベースの活用促進	医療データベースのオンライン化が促進され、効率的に情報収集や参照が行えるようになる。

# ステークホルダー別の導入効果③

- 医療等分野サービスへの接続や地域医療連携ネットワーク間の相互接続を行うために、**医療機関等が個別にネットワークを整備するのではなく、相互接続基盤を利用することで全体で多くのネットワーク費用の適正化効果**が見込まれる。
- また、情報共有の円滑化により、重複検査・処方削減も見込まれるため、**医療費の適正化**に寄与する可能性有。

ステークホルダー	導入効果	試算方法（前提条件）	導入効果		
			医療等分野のサービス普及率の推計を基に 試算した施設数が相互接続基盤を利用した場合		全ての施設が相互接続基盤 を利用した場合
			平成32年度 (運用開始初年度を想定)	平成37年度 (運用開始5年後を想定)	
医療機関等 (病院、医科・歯科診療所、薬局)	②回線統合・クラウド化促進に伴うICTコスト・管理の最適化	<b>【ネットワーク費用の適正化効果】</b> ・「オンライン請求」、「地域医療連携NW」、「民間サービス（例：クラウド型電子カルテ）」利用にあたり、ネットワークを個別に敷設する場合（最大3回線）と相互接続基盤に回線1本を敷設し、各サービスを利用する場合の整備費用から適正化効果を試算	<b>【イニシャル費用】</b> ・約46億円の削減 ※病院：約2億、医科診療所：約19億、歯科診療所：約6億、薬局：約19億  <b>【ランニング費用（年間）】</b> ・約194億円の削減 ※病院：約7億、医科診療所：約83億、歯科診療所：約25億、薬局：約80億	<b>【イニシャル費用】</b> ・約62億円の削減 ※病院：約2億、医科診療所：約29億、歯科診療所：約11億、薬局：約20億  <b>【ランニング費用（年間）】</b> ・約266億円の削減 ※病院：約9億、医科診療所：約123億、歯科診療所：約48億、薬局：約86億	<b>【イニシャル費用】</b> ・約112億円の削減 ※病院：約3億、医科診療所：約48億、歯科診療所：約34億、薬局：約28億  <b>【ランニング費用（年間）】</b> ・約478億円の削減 ※病院：約12億、医科診療所：約203億、歯科診療所：約144億、薬局：約119億
患者	⑥医療費の適正化	・外来における重複検査・処方の医療費と、医療情報連携ネットワーク間で診療情報が連携されることによる重複検査・処方の削減率を各種調査事例から推計し、医療費の適正化効果を試算  ※相互接続基盤構築によってEHRによる施設間の情報連携が促進されると仮定した場合の効果	<b>数十億円程度（年間）の適正化効果</b>  外来重複医療費について各種調査事例から推計し、総務省健康情報活用基盤構築事業（平成23～24年度）のアンケート結果等を用いて、仮に重複検査、重複投薬を削減できた場合の推計。		<b>数百億円程度（年間）の適正化効果</b>

# 事業主体の要件

- **相互接続基盤を運用する事業主体が整備されていることが必須。**
- 相互接続基盤の役割を踏まえると、「**公共性・透明性**」、「**事業継続性**」、「**組織の意思決定**」、「**情報セキュリティ**」、「**サービス/品質**」、「**接続事業者評価**」及び「**電気通信事業**」の要件を担保できる事業主体を選定する必要有。

## □ 公共性・透明性

- ✓ 公共のサービス主体が運営しているといった意識（社会性）をステークホルダが持つことが、より多くの医療機関等の参加を促すことが期待できることから、公共性をもった事業主体が望ましい。
- ✓ 社会性を担保するためには、法人の運営について透明性の確保が重要となる。法人のガバナンスを有効に機能させる仕組みが必要である。
- ✓ 運用に関する監査が行われること。

## □ 事業継続性

- ✓ 想定するビジネスモデルにより、初期導入コストだけでなく、サービスを維持するためのコスト（運用コスト）の調達をどこから調達し、誰が負担するか、また負担に関して理解が得られるかの検討、定義が必要である。

## □ 組織の意思決定

- ✓ 運営組織内において厳格な意思決定のルールを定めて運用することが重要となる。一部のステークホルダのみが有利とならないように意思決定の公共性が担保するガバナンスの設計が必要である。

## □ 情報セキュリティ

- ✓ 相互接続基盤を流れる情報は、医療情報を含むことから、より高度な安全性が要求される。情報セキュリティの対策が十分にできる運営体制の構築が必要である。
- ✓ 事業主体が認証（例えば、ISMS、プライバシーマーク等）を受けていること。

## □ サービス/品質

- ✓ サービスおよび品質については、相互接続基盤の公共性から、サービス提供者に対して公平に提供する。
- ✓ 相互接続基盤の構築、安定運用においては、必要なスキルを持った技術要員の確保が必要である。

## □ 接続事業者評価

- ✓ 相互接続基盤に接続する事業者が、特定の事業者のみに限定しない客観的な評価を、相互接続基盤の運営主体が行うこと。また、評価は、外部への委託も可能にすること。

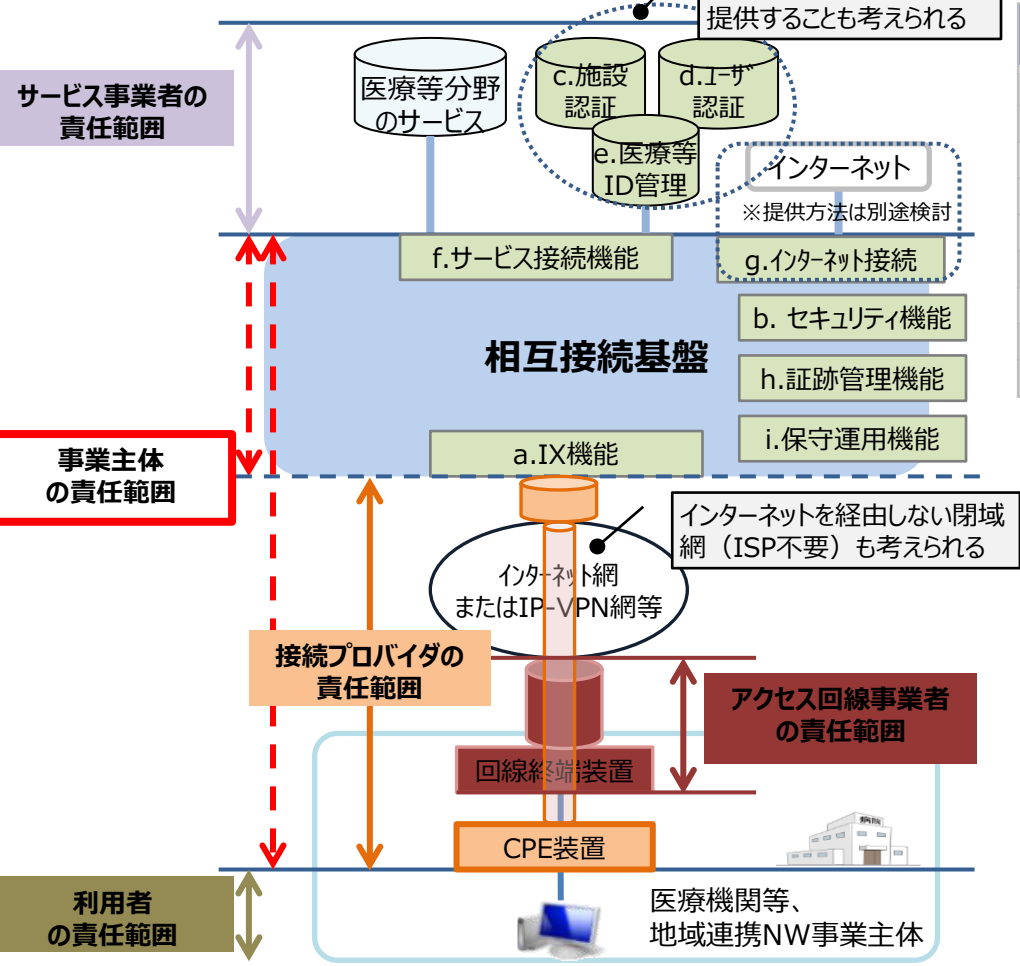
## □ 電気通信事業

- ✓ 電気通信事業法に基づく行政への「届出」を行い、電気通信事業者となること。
- ✓ 「電気通信事業法」、「電気通信事業における個人情報保護に関するガイドライン」等の法令・ガイドラインを順守すること。

# 事業主体の責任範囲及び提供機能

- 事業主体の責任範囲は、**相互接続基盤に限定した方式（利用者との契約は接続プロバイダが担う）と相互接続基盤までの接続サービスを含める方式（利用者との契約も基本的に事業主体が担う）**の2パターンを想定。
- 各機能の提供主体は異なる可能性はあるが、全ての機能が必須機能であり、そのうち、相互接続基盤の役割を鑑みると、**事業主体は、「a.IX機能」、「b.セキュリティ機能」、「f.サービス接続機能」、「h.証跡管理機能」、「i.保守運用機能」**を提供する必要有。

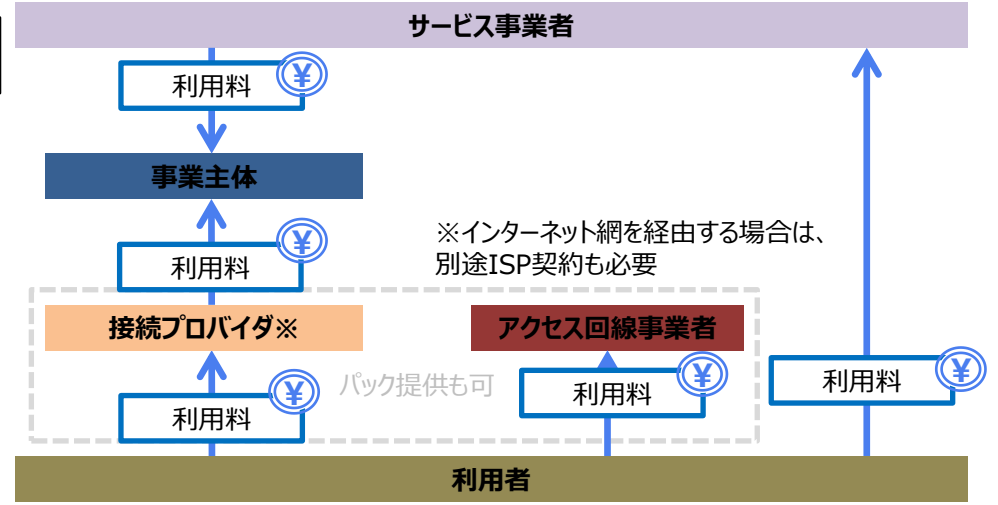
## ■ 事業主体の責任範囲



## ■ 医療等分野で必要な機能及び事業主体による提供必須機能

機能一覧	機能概要	事業主体による提供必須機能
a.IX機能	接続プロバイダの相互接続性を提供	●
b.セキュリティ機能	相互接続基盤のセキュリティ対策	●
c.施設認証機能	医療機関等の施設認証	要検討
d.ユーザ認証機能	医療従事者等の利用者認証	要検討
e.医療等ID管理	医療等IDを管理する機能（発番機能は除く）	要検討
f.サービス接続機能	サービス事業者の接続	●
g.インターネット接続機能	診療等に必要な限定サイトを接続する機能	要検討
h.証跡管理機能	相互接続基盤の通信ログを取得・管理	●
i.保守運用機能	ヘルプデスク、障害復旧、利用者管理	●

## ■ 契約形態（例）



# 利用料負担モデルの検討

- 様々な前提条件が未決定であり、費用の試算（推計）を行うのは非常に難しいが、これまで検討してきた事業主体に必要な要件などを仮置きして試算（推計）した。その結果、条件により大きく変動する可能性があるが、相互接続基盤に係る概算費用(事業主体運営費を含む)は、インシャル費用が30～60億円程度、ランニング費用が年間15～25億円程度と試算（推計）した。なお、特にセキュリティ対策の方法、範囲等について、更に検討が必要であり、その結果、インシャル費用、ランニング費用ともに大きく異なる結果となる可能性がある。
- 相互接続基盤の安定した事業運営を踏まえると、医療機関等がある程度確保できるまでの間、**行政機関等による事業費の支援を検討する必要有**。有識者からも、**行政機関等による具体的な支援の検討が望ましい**との意見有。
  - 重複投薬削減効果に基づき**受益者となる行政機関や保険者等による相互接続基盤の費用一部負担の検討すべき**。
  - 最終的には受益者負担モデルを目指すとしても、**初期段階は、国の財源等による早期立上げが必要**。また、行政機関等による地域医療連携NWに係る**補助金割当は、相互接続基盤を用いることを前提条件とする**等、効果的な仕組みを検討すべき。

	利用料負担モデル	メリット	デメリット
医療機関等による負担	①一律に設定	<ul style="list-style-type: none"> <li>一律に負担するため、事業主体の事務負担が簡素化される</li> <li>想定される施設数から確保できる利用料を想定できる</li> </ul>	<ul style="list-style-type: none"> <li>相互接続基盤の利用料によっては、負担できない利用者が発生する可能性がある（普及促進の阻害要因になる可能性がある）</li> </ul>
	②利用するネットワークサービス毎に利用料を設定	<ul style="list-style-type: none"> <li>利用者自身が利用料を選択できる</li> <li>ネットワークサービス毎に相互接続基盤の利用料を決定するため、事業主体の事務負担が簡素化される</li> </ul>	<ul style="list-style-type: none"> <li>ネットワークサービスの一般的な料金設定方法であり、大きなデメリットは想定しにくい</li> </ul>
	③流通する情報量を基に利用料（従量課金）を設定	<ul style="list-style-type: none"> <li>相互接続基盤を多く利用する利用者の負担料が多くなるため、利用者の公平性が担保される</li> </ul>	<ul style="list-style-type: none"> <li>相互接続基盤を流通する情報のパケット量を監視するための設備投資が必要となる</li> <li>流通する情報量の実績により利用料が変わるため、事業主体の事務作業が煩雑化する</li> </ul>
	④医療等分野のサービス利用数を基に利用料（従量課金）を設定	<ul style="list-style-type: none"> <li>回線費用の削減等のメリットを享受できる利用者が多く負担するため、利用者の公平性が担保される</li> </ul>	<ul style="list-style-type: none"> <li>利用するサービス数により利用料が異なるため、事業主体の事務作業負担が煩雑化する</li> </ul>
	⑤施設分類・病床規模を考慮し、利用料を設定	<ul style="list-style-type: none"> <li>医療機関等の負担能力に応じて利用料を設定するため、相互接続基盤の普及促進に繋がる可能性がある</li> <li>利用が想定される施設数から確保できる利用料を想定できる</li> </ul>	<ul style="list-style-type: none"> <li>施設分類・病床規模により利用料が異なるため、事業主体の事務作業が煩雑化する</li> <li>施設分類・病床規模に関わらず利用できるサービスは変わらないため、利用者の公平性が担保されない</li> </ul>
公的資金による負担	⑥公的資金による一部負担	<ul style="list-style-type: none"> <li>医療機関等の費用負担が軽減され、医療機関は相互接続基盤を利用しやすくなる。</li> </ul>	<ul style="list-style-type: none"> <li>医療機関等へのデメリットはないが、公的資金の財源確保に伴う検討・調整に長期間を有することが想定される</li> </ul>
サービス事業者による負担	⑦サービス事業者に対して利用するネットワークサービス毎に利用料を設定	<ul style="list-style-type: none"> <li>医療機関等の費用負担が軽減され、医療機関は相互接続基盤の利用しやすくなる。</li> <li>複数のサービスが提供されることで医療機関等にとっての価値が高まり、利用促進を期待できる</li> </ul>	<ul style="list-style-type: none"> <li>医療等分野サービスを提供するサービス事業者を確保する施策の検討が必要である</li> </ul>

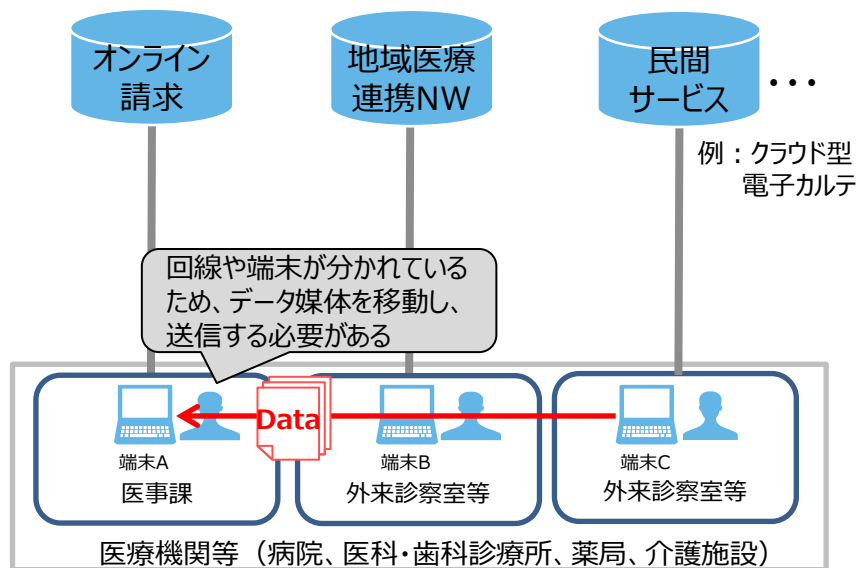


# 施設分類別の導入効果と負担（ヒアリング結果を踏まえた導入効果）

- 実証フィールドのヒアリング結果を踏まえると、**回線毎に分断されている業務の解消、外部との医療情報共有・連携に対するセキュリティの確保、回線統合による回線・端末費用の削減、共同利用によるクラウドサービスの利用推進**の効果有。
- 病院、診療所、薬局については、接続にかかる一定の負担がかかるものの、導入効果が認められるが、歯科、介護施設については、電子化が進み、院外とやりとりする利用シーンが発生すれば、導入効果が認められる可能性有。

## 将来（2025年）を例に、相互接続基盤の整備有無による効果と負担を測定

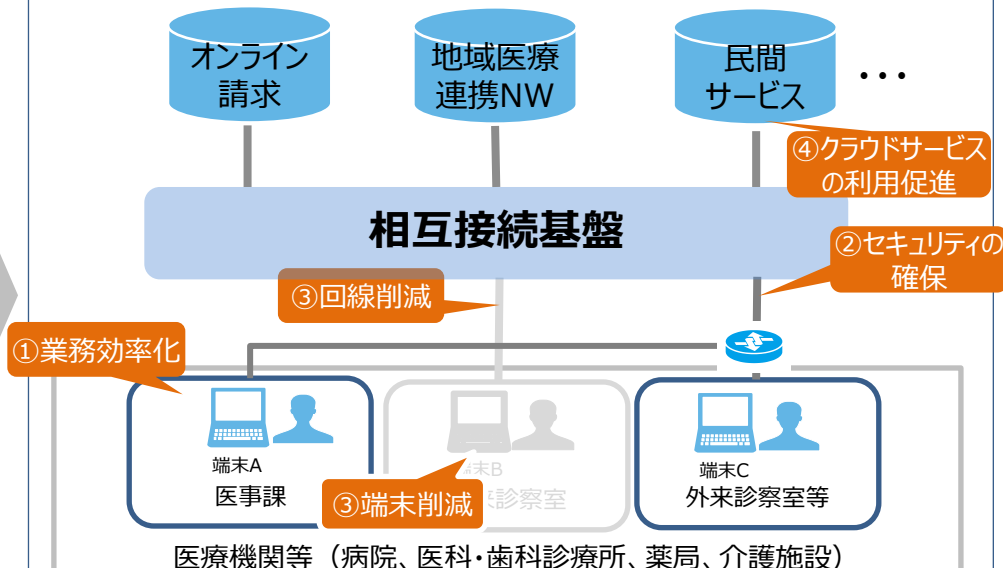
相互接続基盤が整備されない場合（例：2025年）



### 課題

- 今後、様々な医療等分野サービスが普及するに伴い、用途別に回線や端末を敷設する可能性がある。
- 用途別に回線や端末を敷設すると、システム間のデータ移動（USB等）や情報のコピー＆ペーストの手間が発生し、業務が煩雑になり、診療業務に支障をきたすことが想定される。

相互接続基盤が整備された場合（例：2025年）



### 導入効果

#### 【安心安全な医療情報共有・連携による診療業務の効率化】

- ① 回線毎に分断されている業務の解消
  - ② 外部との医療情報共有・連携に対するセキュリティの確保
- #### 【回線統合・クラウド化促進に伴うICTコスト・管理の最適化】
- ③ 回線統合による回線・端末費用の削減

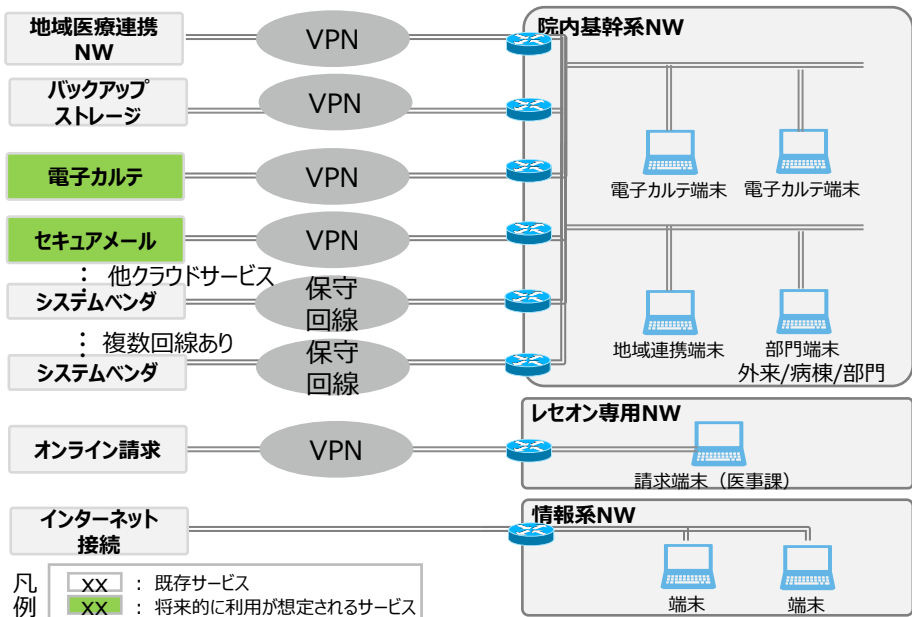
※将来的な相互接続基盤を介したサービス増加によりさらに削減効果見込

- ④ 共同利用によるクラウドサービスの利用促進

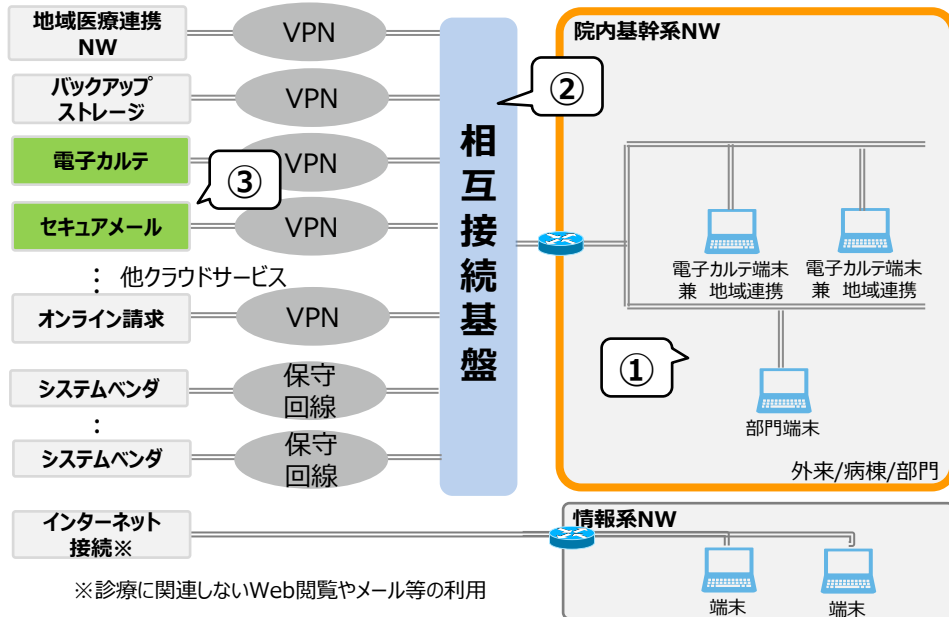
# 施設分類別の導入効果と負担（病院における試算）

- ・ 沖縄フィールドにおける実際の病院NW構成を踏まえ、**病院における導入効果と負担を検証**。
- ・ 接続にかかる一定の負担がかかるものの、**利便性やセキュリティの向上、回線や端末の集約効果有**と想定。

相互接続基盤が整備されない場合（例：2025年）



相互接続基盤が整備された場合（例：2025年）



## 接続による導入効果

- ※300床規模の中規模病院を想定、端末は約500台を想定
- ※回線集約：IP-VPN 9.7千円/月（回線）と想定
- ※端末集約：オンライン請求用1台、地連5台と想定
- ※業務効率：NW管理・変更稼働30時間/年と想定

### 【定量効果】

項目	費用（年）	内容
回線集約	70万円	7回線を1回線に集約
端末集約、業務効率等	37万円	端末6台集約、5年償却
合計	107万円	

### 【定性効果】

- ・ 業務分断が解消され、各サービスを一連で利用可能になる（右上図①）
- ・ 安心して院外との情報連携が可能になる（右上図②）
- ・ 共同利用により安価で均一なクラウドサービスの利用が可能になる（右上図③）

## 接続に係る負担

- ※回線は、IP-VPN相当を利用済、基幹系と情報系は分離を前提
- ※ルータ設置・端末設定で約100万を想定
- ※端末設定は、DGW・DNS設定等にかかる費用

### 【導入・運用費】

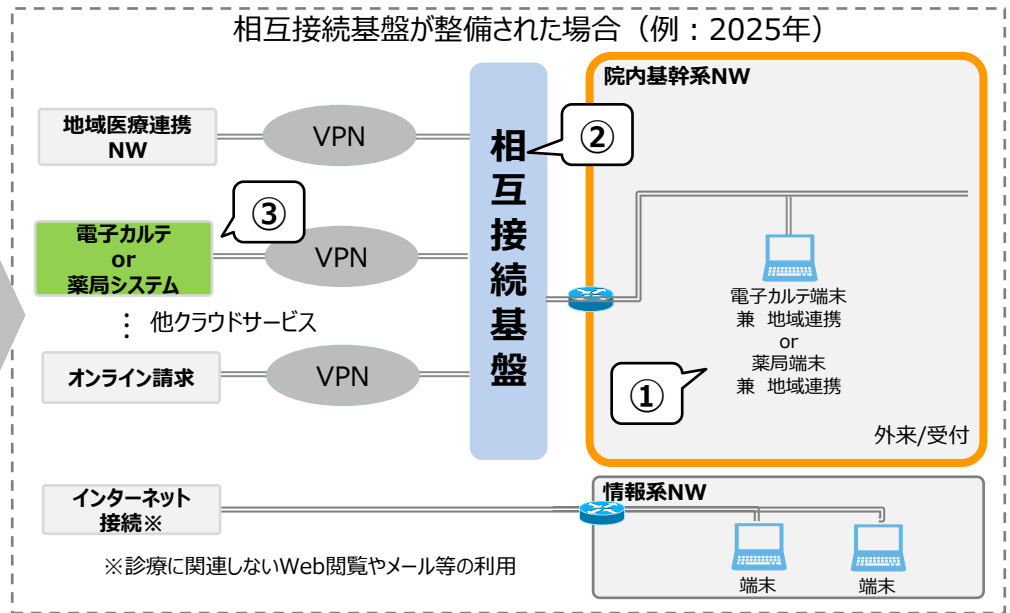
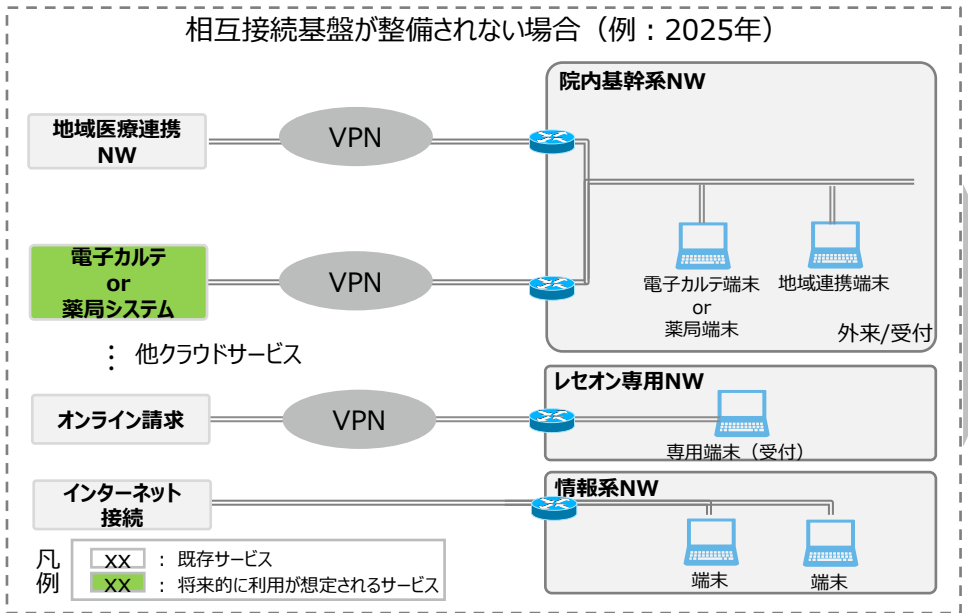
項目	費用（年）	内容
接続料	未定	—
ルータ設置・端末設定	20万円	5年償却

## 総合評価

- ・ 業務分断解消による利便性向上や安心して院外との情報連携が可能になる
- ・ 回線や端末の集約等により、87万円/年（7.2万円/月）のコスト削減効果（回線の削減効果は、約60%見込）※接続料は含まない

# 施設分類別の導入効果と負担（診療所・薬局における試算）

● 沖縄フィールドにおける実際の診療所・薬局NW構成を踏まえ、**診療所・薬局における導入効果と負担を検証**。  
 ● **利便性やセキュリティの向上**に加え、利用するサービス数が増えれば、**回線や端末の集約効果が高くなる**。



## 接続による導入効果

※診療所・薬局の端末は約20台と想定  
 ※回線集約：IP-VPN 9.7千円/月（回線）と想定  
 ※端末集約：オンライン請求用1台、地連2台と想定  
 ※業務効率は、回線やNW設定変更がほぼないため想定しない

### 【定量効果】

項目	費用（年）	内容
回線集約	30万円	3回線を1回線に集約
端末集約	6万円	端末3台集約、5年償却
合計	36万円	

### 【定性効果】

- 業務分断が解消され、各サービスを一連で利用可能になる（右上図①）
- 安心して院外との情報連携が可能になる（右上図②）
- 共同利用により安価で均一なクラウドサービスの利用が可能になる（右上図③）

## 接続に係る負担

※回線は、IP-VPN相当を利用済、基幹系と情報系は分離を前提  
 ※ルータ設置・端末設定で約20万を想定  
 ※端末設定は、DGW・DNS設定等にかかる費用

### 【導入・運用費】

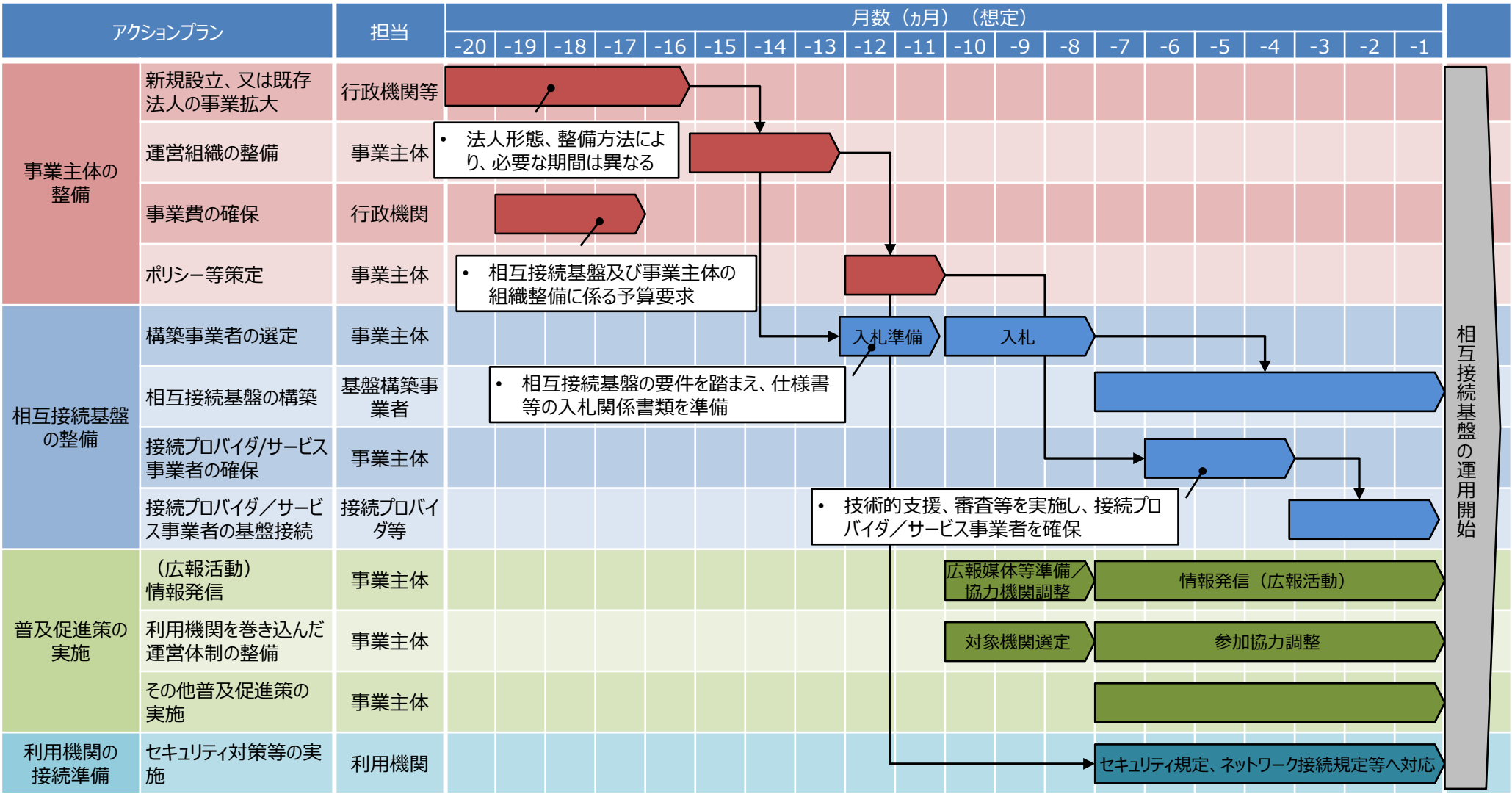
項目	費用（年）	内容
接続料	未定	—
ルータ設置・端末設定	4万円	5年償却

## 総合評価

- 業務分断解消による利便性向上や安心して院外との情報連携が可能になる
- 回線や端末集約により、32万円/年（2.6万円/月）のコスト削減効果、利用するサービス数が増えれば、集約効果が高くなる（回線の削減効果は、約60%見込）※接続料は含まない

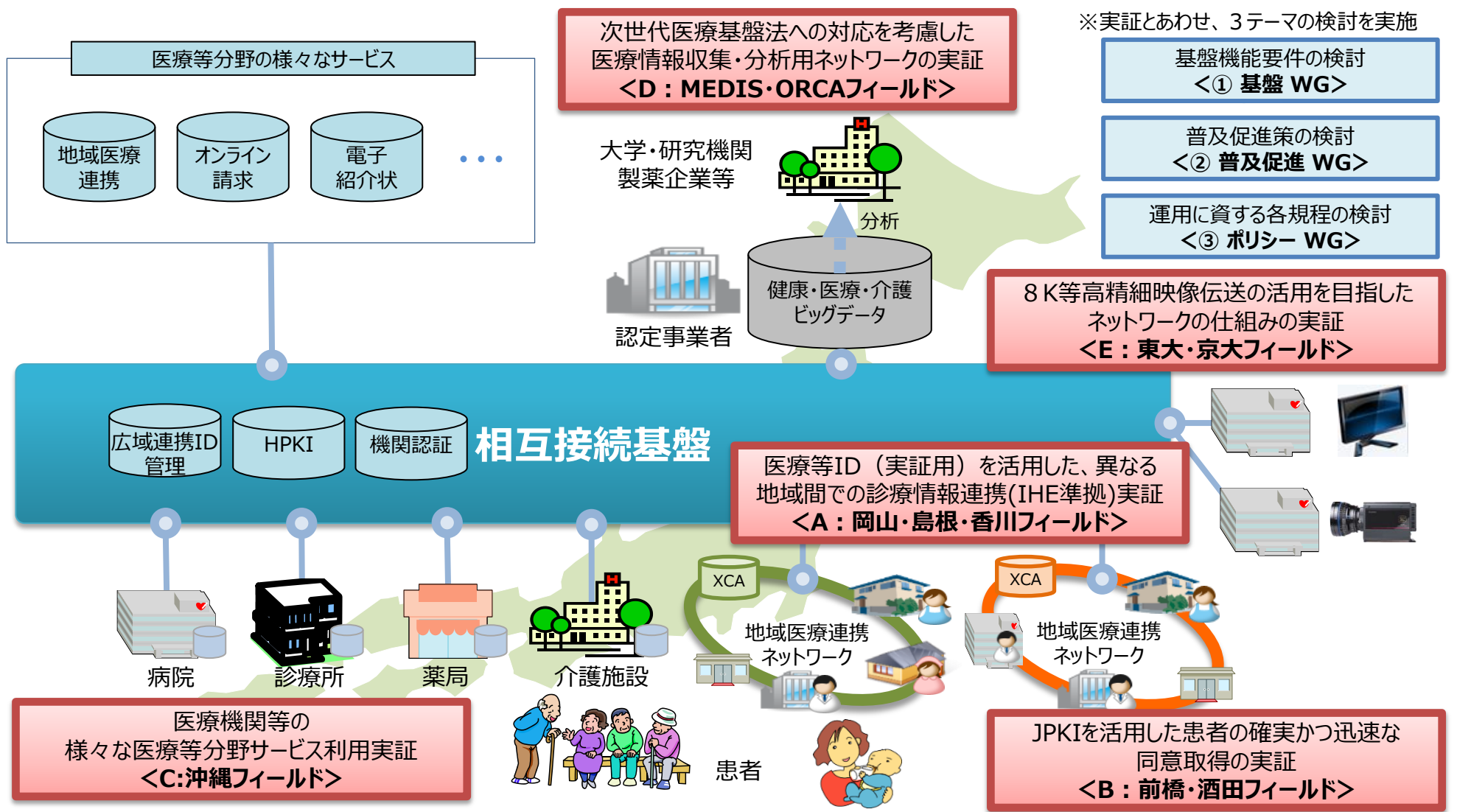
# スケジュール（想定）

事業主体の法人形態や整備方法、及び相互接続基盤が提供する機能に依存するが、現時点では相互接続基盤の運用開始までの準備期間として**1年8カ月程度**の見込。



# 相互接続基盤モデルの実証フィールド

- テーマ別に3つの検討WG「①基盤」、「②普及促進」、「③ポリシー」、および、5つのフィールド実証WG「A:岡山・島根・香川」、「B:前橋・酒田」、「C:沖縄」、「D:MEDIS・ORCA」、「E:東大・京大」にて、検証を実施。



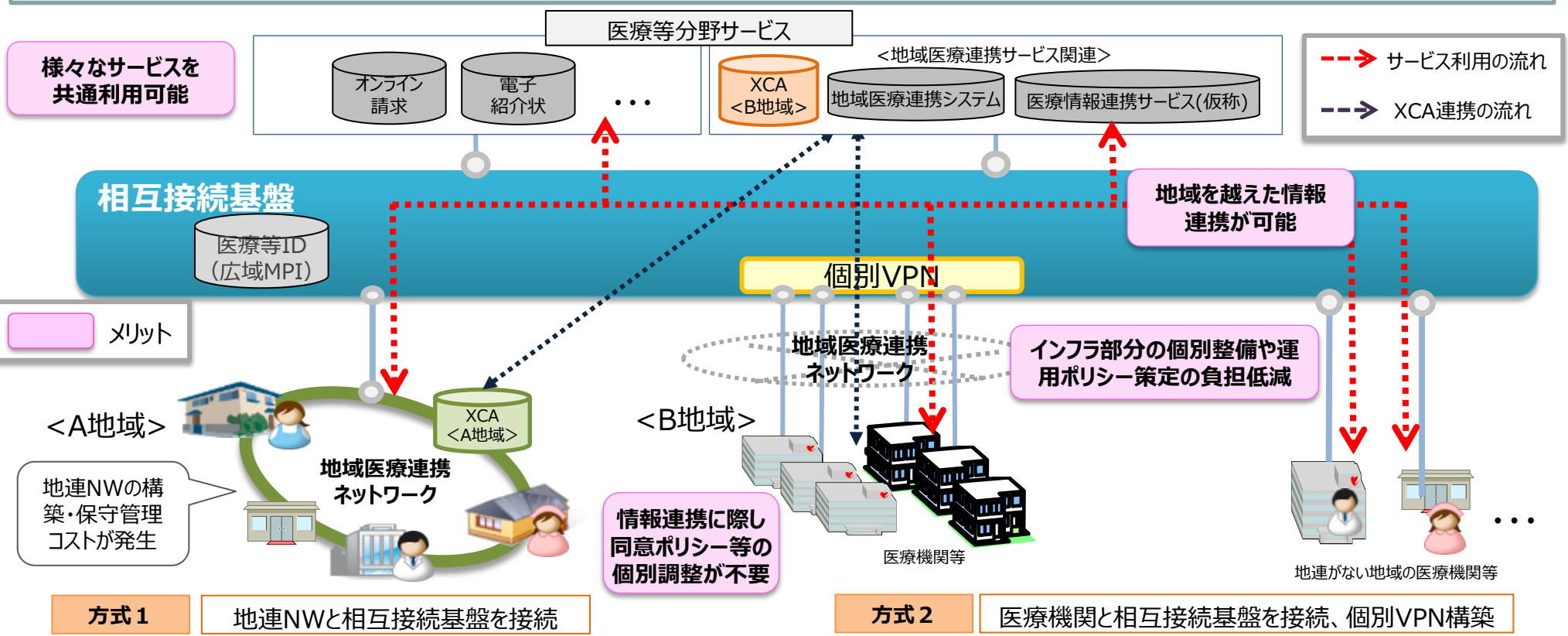
# A : 岡山・島根・香川フィールド成果

## <主な成果>

- 相互接続基盤が、**地域を越えた診療情報の連携を実現するうえで有効**であることを示すとともに、標準準拠の情報連携（IHE準拠のXCA連携）に必要な事項を整理（異なる地域間でのIHE準拠の診療情報連携の実施は我が国初）。
- 地域医療連携ネットワークからみた相互接続基盤のメリットは、「他地域との情報連携に際し同意ポリシー等の個別調整が不要」、「様々なサービスの共通利用が可能」、「インフラ部分の個別整備や運用ポリシー策定の負担が低減」の3点。
- 単に隣接する地域医療連携ネットワーク間で連携するだけではない全国規模の情報連携の際には、「セキュリティポリシー・責任分界点整理」、「患者同意・撤回取得方法」、「利用者管理・認証方法」、「連携する情報項目・表示方法」等の**全国に適用可能なルールの策定（制度化等）**が必要であり、その考え方を整理した。

## <今後の課題>

- 全国規模の情報連携では、「全国に適用可能なルールの具体化」等が課題。



# B : 前橋・酒田フィールド成果

## <主な成果>

- JPKIを用いて、「**確実な本人確認**」、「**即時の同意取得**」、「**誤りのない患者情報紐付け**」を実施し、有効なモデルを示した。
- 診療現場において、マイナンバーカードのJPKI署名を用いた患者確認、患者同意による受診履歴と診療情報の紐付け登録、HPKIとJPKIを用いた医師への受診履歴と診療情報の開示までを確認し、技術課題を抽出。
- 「患者受診履歴」を活用した簡易な診療情報連携のモデルを提示。

## <今後の課題>

- 受診履歴と診療情報の紐付け登録時における、**医師および患者の運用負担軽減**が課題。  
負担軽減策として、初回のみ同意取得や、受付窓口等での実施などの運用を検討。



確実な本人確認  
即時の同意取得  
誤りのない患者情報紐付け

確実な本人確認  
即時の同意取得  
誤りのない患者情報紐付け

登録側

参照側

<受付窓口等>

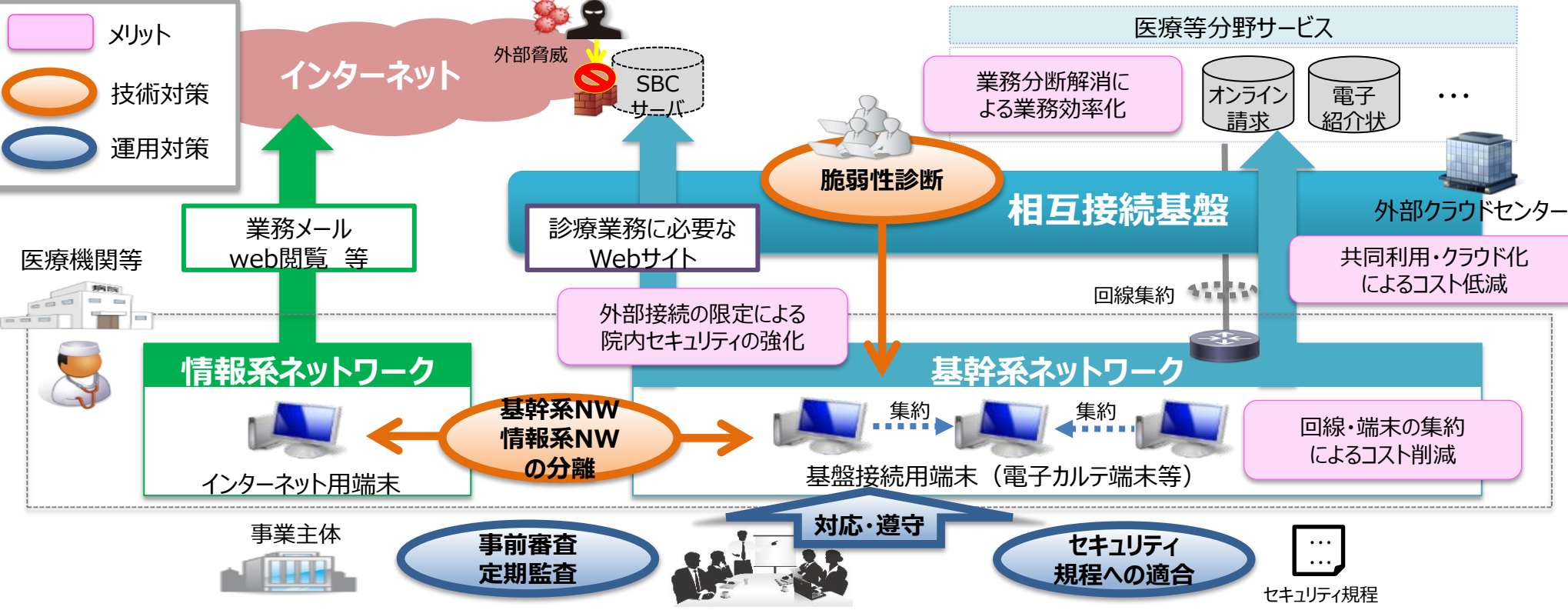
# C : 沖縄フィールド成果

## <主な成果>

- 医療機関等が相互接続基盤を介して様々なサービスを利用するユースケース実証やヒアリングを通じ、**各施設分類別**に相互接続基盤の**導入効果および必要となる費用や負担**を抽出。
- 医療機関等からみた相互接続基盤のメリットは、「業務分断の解消、基幹系ネットワークから様々な外部サービスを共通利用することによる業務効率化」、「統一ポリシーに基づき一定のセキュリティレベルが確保された相互接続基盤のみに外部接続が限定され、院内セキュリティが強化」、「回線・端末の統合効果によるコスト削減」、「今後、相互接続基盤上で共同利用によるクラウドサービスが提供されることによるシステムコスト低減」の4点。

## <今後の課題>

- 相互接続基盤への接続にあたって、医療機関等の費用負担は比較的低廉と見込まれるが、現行、基幹系と情報系ネットワークを共用している医療機関等について、**ネットワーク分離やセキュリティ規程への適合対応等が必要。**





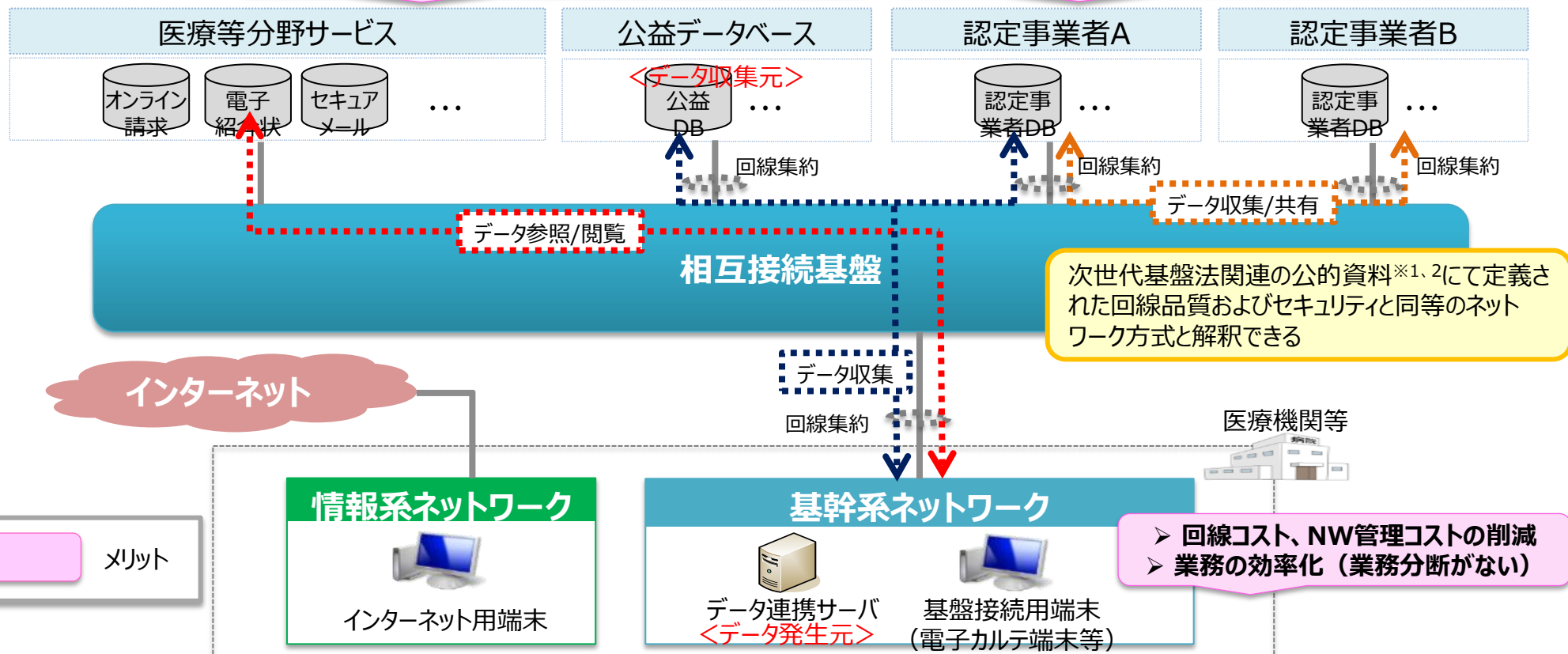
# D : MEDIS・ORCAフィールド成果

## <主な成果>

- 相互接続基盤によって、統一ポリシーに基づき運用され、一定のセキュリティレベルが確保されることで、**診療情報収集・分析における普及の後押し**となる。
- 「認定匿名加工医療情報作成事業者」と、「データ収集元」、「データ発生元」、「データ提供先」の間を相互接続基盤を介して接続し、**複数のネットワークの方式案を検討**し、「コスト・負担面」等で評価。

➤ 回線コスト、NW管理コストの削減

➤ 回線コスト、NW管理コストの削減  
➤ 接続ポリシー統一による運用負担軽減



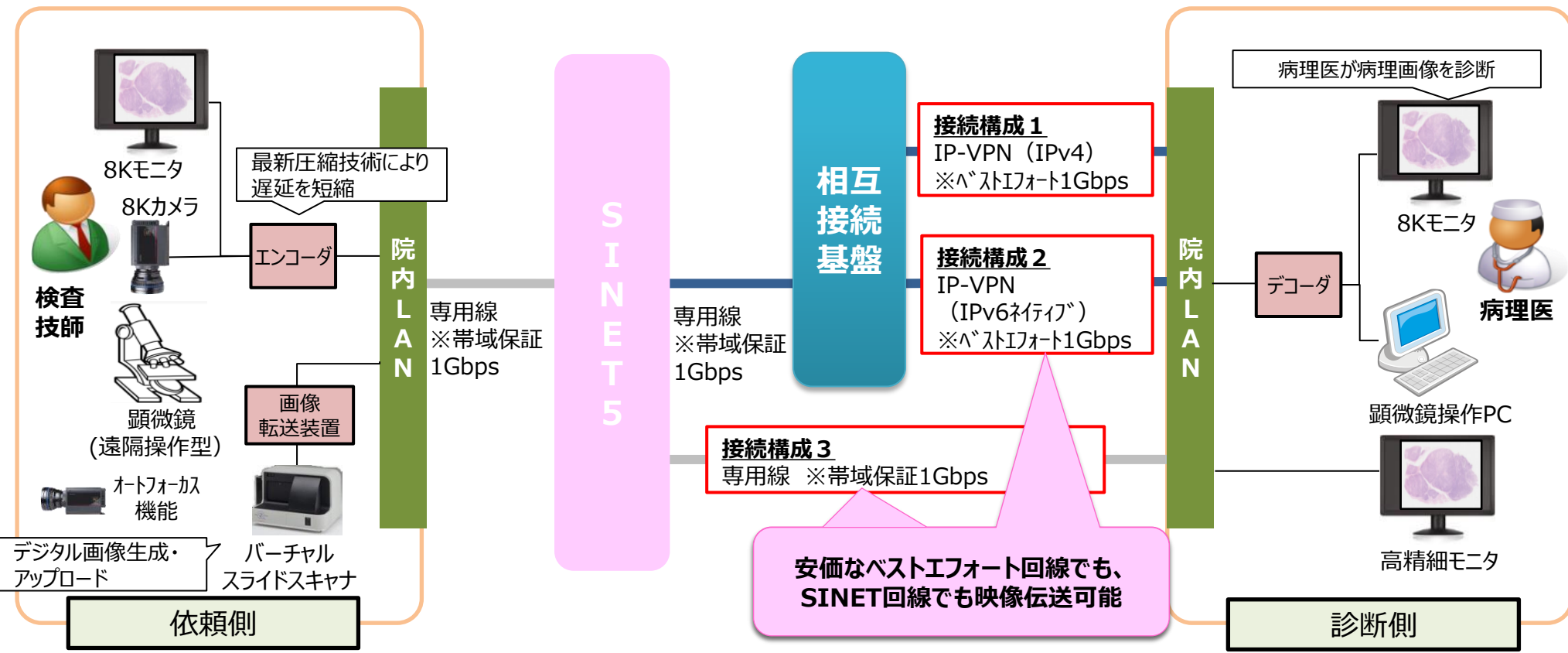
※1 平成30年3月9日に内閣官房健康・医療戦略室より公示された「医療分野の研究開発に資するための匿名加工医療情報に関する法律についてのガイドライン」

※2 平成30年1月24日の第5回 次世代医療ICT基盤協議会で配布された「次世代医療基盤法の施行に向けた検討の状況について」

# E : 東大・京大フィールド成果

## <主な成果>

- 相互接続基盤を介して、遠隔病理診断における2つのユースケース「① 8 K映像圧縮伝送（リアルタイム伝送）」、「②バーチャルスライドスキャナ画像共有（非リアルタイム伝送）」を実証し、それぞれの利用形態でのネットワーク要件を整理。
- **8 K等大容量データを扱う場合においても、医療機関等は安価なベストエフォート回線を接続して相互接続基盤経由で利用可能。また、大学病院等の既設のSINETを用いても同様に可能。**
- 顕微鏡を用いた8 K圧縮映像伝送による遠隔病理診断は、システム性能や操作性において高い評価。



「8 K圧縮映像伝送」「バーチャルスライドスキャナ画像共有」の構成